

33 CFR
Navigation and Navigable Waters

CHAPTER I

**COAST GUARD, DEPARTMENT OF
HOMELAND SECURITY**

SUBCHAPTER H -- MARITIME SECURITY

Part 101—Maritime Security: General

Part 103—Maritime Security: Area Maritime Security

Part 104—Maritime Security: Vessels

Part 105—Maritime Security: Facilities

**Part 106—Maritime Security: Outer Continental
Shelf (OCS) Facilities**

As amended by the Final Rules

<http://www.gpoaccess.gov/fr/index.html>

Part 101: USCG-2003-14792, 68 FR 60447, October 22, 2003

Part 103: USCG-2003-14733, 68 FR 60471, October 22, 2003

Part 104: USCG-2003-14749, 68 FR 60482, October 22, 2003

Part 105: USCG-2003-14732, 68 FR 60514, October 22, 2003

Part 106: USCG-2003-14759, 68 FR 60558, October 22, 2003

33 CFR
Navigation and Navigable Waters
CHAPTER I
COAST GUARD, DEPARTMENT
OF HOMELAND SECURITY
SUBCHAPTER H -- MARITIME
SECURITY

PART 101—
MARITIME SECURITY:
GENERAL

Subpart A -- General

Sec.

- 101.100 Purpose.
- 101.105 Definitions.
- 101.110 Applicability.
- 101.115 Incorporation by reference.
- 101.120 Alternatives.
- 101.125 Approved Alternative Security Programs.
- 101.130 Equivalent security measures.

Subpart B -- Maritime Security
(MARSEC) Levels

- 101.200 MARSEC Levels.
- 101.205 Department of Homeland Security alignment.

Subpart C -- Communication (Port-Facility-Vessel)

- 101.300 Preparedness communications.
- 101.305 Reporting.
- 101.310 Additional communication devices.

Subpart D -- Control Measures for Security

- 101.400 Enforcement.
- 101.405 Maritime Security (MARSEC) Directives.
- 101.410 Control and Compliance Measures.
- 101.415 Penalties.
- 101.420 Right to appeal.

Subpart E -- Other Provisions

- 101.500 Procedures for authorizing a Recognized Security Organization (RSO).

[RESERVED]

- 101.505 Declaration of Security (DoS).
- 101.510 Assessment Tools.
- 101.515 Personal Identification.

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. Chapter 701; 50 U.S.C. 191, 192; Executive Order 12656, 3 CFR 1988 Comp., p. 585; 33 CFR 1.05–1, 6.04–11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No. 0170.1.

Source: USCG–2003–14792, 68 FR 39278, July 1, 2003.

Subpart A—General

§ 101.100 Purpose.

(a) The purpose of this subchapter is:

(1) To implement portions of the maritime security regime required by the Maritime Transportation Security Act of 2002, as codified in 46 U.S.C. Chapter 701;

(2) To align, where appropriate, the requirements of domestic maritime security regulations with the international maritime security standards in the International Convention for the Safety of Life at Sea, 1974 (SOLAS Chapter XI–2) and the International Code for the Security of Ships and of Port Facilities, parts A and B, adopted on 12 December 2002; and

(3) To ensure security arrangements are as compatible as possible for vessels trading internationally.

(b) For those maritime elements of the national transportation system where international standards do not directly apply, the requirements in this subchapter emphasize cooperation and coordination with local port community stakeholders, and are based on existing domestic standards, as well as established industry security practices.

(c) The assessments and plans required by this subchapter are intended for use in implementing security measures at various MARSEC Levels. The specific security measures and their implementation are planning criteria based on a set of assumptions made during the development of the security

assessment and plan. These assumptions may not exist during an actual transportation security incident.

§ 101.105 Definitions.

Unless otherwise specified, as used in this subchapter:

Alternative Security Program means a third-party or industry organization developed standard that the Commandant has determined provides an equivalent level of security to that established by this subchapter.

Area Commander means the U.S. Coast Guard officer designated by the Commandant to command a Coast Guard Area as described in 33 CFR part 3.

Area Maritime Security (AMS) Assessment means an analysis that examines and evaluates the infrastructure and operations of a port taking into account possible threats, vulnerabilities, and existing protective measures, procedures and operations.

Area Maritime Security (AMS) Committee means the committee established pursuant to 46 U.S.C. 70112(a)(2)(A). This committee can be the Port Security Committee established pursuant to Navigation and Vessel Inspection Circular (NVIC) 09-02, available from the cognizant Captain of the Port (COTP) or at <http://www.uscg.mil/hq/g-m/nvic>.

Area Maritime Security (AMS) Plan means the plan developed pursuant to 46 U.S.C. 70103(b). This plan may be the Port Security plan developed pursuant to NVIC 09-02 provided it meets the requirements of part 103 of this subchapter.

Area of Responsibility (AOR) means a Coast Guard area, district, marine inspection zone or COTP zone described in 33 CFR part 3.

Audit means an evaluation of a security assessment or security plan performed by an owner or operator, the owner or operator's designee, or an approved third-party, intended to identify deficiencies, non-conformities and/or inadequacies that would render the assessment or plan insufficient.

Barge means a non-self-propelled vessel (46 CFR 24.10-1).

Barge fleeting facility means a

commercial area, subject to permitting by the Army Corps of Engineers, as provided in 33 CFR part 322, part 330, or pursuant to a regional general permit, the purpose of which is for the making up, breaking down, or staging of barge tows.

Breach of security means an incident that has not resulted in a transportation security incident, in which security measures have been circumvented, eluded, or violated.

Bulk or in bulk means a commodity that is loaded or carried on board a vessel without containers or labels, and that is received and handled without mark or count.

Bunkers means a vessel's fuel supply.

Captain of the Port (COTP) means the local officer exercising authority for the COTP zones described in 33 CFR part 3. The COTP is the Federal Maritime Security Coordinator described in 46 U.S.C. 70103(a)(2)(G) and also the Port Facility Security Officer as described in the ISPS Code, part A.

Cargo means any goods, wares, or merchandise carried, or to be carried, for consideration, whether directly or indirectly flowing to the owner, charterer, operator, agent, or any other person interested in the vessel, facility, or OCS facility, except dredge spoils.

Cargo vessel means a vessel that carries, or intends to carry, cargo as defined in this section.

Certain Dangerous Cargo (CDC) means the same as defined in 33 CFR 160.204.

Commandant means the Commandant of the U.S. Coast Guard.

Company means any person or entity that owns any facility, vessel, or OCS facility subject to the requirements of this subchapter, or has assumed the responsibility for operation of any facility, vessel, or OCS facility subject to the requirements of this subchapter, including the duties and responsibilities imposed by this subchapter.

Company Security Officer (CSO) means the person designated by the Company as responsible for the security of the vessel or OCS facility, including implementation and maintenance of the vessel or OCS facility security plan, and

for liaison with their respective vessel or facility security officer and the Coast Guard.

Contracting Government means any government of a nation that is a signatory to SOLAS, other than the U.S.

Cruise ship means any vessel over 100 gross register tons, carrying more than 12 passengers for hire which makes voyages lasting more than 24 hours, of which any part is on the high seas. Passengers from cruise ships are embarked or disembarked in the U.S. or its territories. Cruise ships do not include ferries that hold Coast Guard Certificates of Inspection endorsed for “Lakes, Bays, and Sounds”, that transit international waters for only short periods of time on frequent schedules.

Dangerous goods and/or hazardous substances, for the purposes of this subchapter, means cargoes regulated by parts 126, 127, or 154 of this chapter.

Dangerous substances or devices means any material, substance, or item that reasonably has the potential to cause a transportation security incident.

Declaration of Security (DoS) means an agreement executed between the responsible Vessel and Facility Security Officer, or between Vessel Security Officers in the case of a vessel-to-vessel activity, that provides a means for ensuring that all shared security concerns are properly addressed and security will remain in place throughout the time a vessel is moored to the facility or for the duration of the vessel-to-vessel activity, respectively.

District Commander means the U.S. Coast Guard officer designated by the Commandant to command a Coast Guard District described in 33 CFR part 3.

Drill means a training event that tests at least one component of the AMS, vessel, or facility security plan and is used to maintain a high level of security readiness.

Exercise means a comprehensive training event that involves several of the functional elements of the AMS, vessel, or facility security plan and tests communications, coordination, resource availability, and response.

Facility means any structure or facility of any kind located in, on, under,

or adjacent to any waters subject to the jurisdiction of the U.S. and used, operated, or maintained by a public or private entity, including any contiguous or adjoining property under common ownership or operation.

Facility Security Assessment (FSA) means an analysis that examines and evaluates the infrastructure and operations of the facility taking into account possible threats, vulnerabilities, consequences, and existing protective measures, procedures and operations.

Facility Security Officer (FSO) means the person designated as responsible for the development, implementation, revision and maintenance of the facility security plan and for liaison with the COTP and Company and Vessel Security Officers.

Facility Security Plan (FSP) means the plan developed to ensure the application of security measures designed to protect the facility and its servicing vessels or those vessels interfacing with the facility, their cargoes, and persons on board at the respective MARSEC Levels.

Ferry means a vessel which is limited in its use to the carriage of deck passengers or vehicles or both, operates on a short run on a frequent schedule between two or more points over the most direct water route, other than in ocean or coastwise service.

Foreign vessel means a vessel of foreign registry or a vessel operated under the authority of a country, except the U.S., that is engaged in commerce.

General shipyard facility means--

(1) For operations on land, any structure or appurtenance thereto designed for the construction, repair, rehabilitation, refurbishment, or rebuilding of any vessel, including graving docks, building ways, ship lifts, wharves, and pier cranes; the land necessary for any structures or appurtenances; and the equipment necessary for the performance of any function referred to in this definition; and

(2) For operations other than on land, any vessel, floating drydock, or barge used for, or a type that is usually used for, activities referred to in paragraph (1) of this definition.

Gross register tons (GRT) means

the gross ton measurement of the vessel under 46 U.S.C. chapter 145, Regulatory Measurement. For a vessel measured under only 46 U.S.C. chapter 143, Convention Measurement, the vessel's gross tonnage, ITC is used to apply all thresholds expressed in terms of gross register tons.

Gross tonnage, ITC (GT ITC) means the gross tonnage measurement of the vessel under 46 U.S.C. chapter 143, Convention Measurement. Under international conventions, this parameter may be referred to as "gross tonnage (GT)."

Hazardous materials means hazardous materials subject to regulation under 46 CFR parts 148, 150, 151, 153, or 154, or 49 CFR parts 171 through 180.

Infrastructure means facilities, structures, systems, assets, or services so vital to the port and its economy that their disruption, incapacity, or destruction would have a debilitating impact on defense, security, the environment, long-term economic prosperity, public health or safety of the port.

International voyage means a voyage between a country to which SOLAS applies and a port outside that country. A country, as used in this definition, includes every territory for the internal relations of which a contracting government to the convention is responsible or for which the United Nations is the administering authority. For the U.S., the term "territory" includes the Commonwealth of Puerto Rico, all possessions of the United States, and all lands held by the U.S. under a protectorate or mandate. For the purposes of this subchapter, vessels solely navigating the Great Lakes and the St. Lawrence River as far east as a straight line drawn from Cap des Rosiers to West Point, Anticosti Island and, on the north side of Anticosti Island, the 63rd meridian, are considered on an "international voyage" when on a voyage between a U.S. port and a Canadian port.

ISPS Code means the International Ship and Port Facility Security Code, as incorporated into SOLAS.

Maritime Security (MARSEC) Directive means an instruction issued

by the Commandant, or his/her delegatee, mandating specific security measures for vessels and facilities that may be involved in a transportation security incident.

Maritime Security (MARSEC) Level means the level set to reflect the prevailing threat environment to the marine elements of the national transportation system, including ports, vessels, facilities, and critical assets and infrastructure located on or adjacent to waters subject to the jurisdiction of the U.S.

MARSEC Level 1 means the level for which minimum appropriate protective security measures shall be maintained at all times.

MARSEC Level 2 means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a transportation security incident.

MARSEC Level 3 means the level for which further specific protective security measures shall be maintained for a limited period of time when a transportation security incident is probable or imminent, although it may not be possible to identify the specific target.

Master means the holder of a valid license that authorizes the individual to serve as a Master, operator, or person in charge of the rated vessel. For the purposes of this subchapter, Master also includes the Person in Charge of a MODU, and the operator of an uninspected towing vessel.

OCS Facility means any artificial island, installation, or other complex of one or more structures permanently or temporarily attached to the subsoil or seabed of the OCS, erected for the purpose of exploring for, developing or producing oil, natural gas or mineral resources. This definition includes all mobile offshore drilling units (MODUs) not covered under part 104 of this subchapter, when attached to the subsoil or seabed of offshore locations, but does not include deepwater ports, as defined by 33 U.S.C. 1502, or pipelines.

Operator, Uninspected Towing Vessel means an individual who holds a license described in 46 CFR

15.805(a)(5) or 46 CFR 15.810(d).

Owner or operator means any person or entity that owns, or maintains operational control over, any facility, vessel, or OCS facility subject to this subchapter. This includes a towing vessel that has operational control of an unmanned vessel when the unmanned vessel is attached to the towing vessel and a facility that has operational control of an unmanned vessel when the unmanned vessel is not attached to a towing vessel and is moored to the facility; attachment begins with the securing of the first mooring line and ends with the casting-off of the last mooring line.

Passenger vessel means—

(1) On an international voyage, a vessel carrying more than 12 passengers including at least one passenger-for-hire; and

(2) On other than an international voyage:

(i) A vessel of at least 100 gross register tons carrying more than 12 passengers, including at least one passenger-for-hire;

(ii) A vessel of less than 100 gross register tons carrying more than 6 passengers, including at least one passenger-for-hire;

(iii) A vessel that is chartered and carrying more than 12 passengers;

(iv) A submersible vessel that is carrying at least one passenger-for-hire; or

(v) A wing-in-ground craft, regardless of tonnage, that is carrying at least one passenger-for-hire.

Passenger-for-hire means a passenger for whom consideration is contributed as a condition of carriage on the vessel, whether directly or indirectly flowing to the owner, charterer, operator, agent, or any other person having an interest in the vessel.

Public access facility means a facility--

(1) That is used by the public primarily for purposes such as recreation, entertainment, retail, or tourism, and not for receiving vessels subject to part 104;

(2) That has minimal infrastructure for servicing vessels subject to part 104 of this chapter; and

(3) That receives only:

(i) Vessels not subject to part 104 of this chapter, or

(ii) Passenger vessels, except:

(A) Ferries certificated to carry vehicles;

(B) Cruise ships; or

(C) Passenger vessels subject to SOLAS Chapter XI.

Registered length means the registered length as defined in 46 CFR part 69.

Restricted areas mean the infrastructures or locations identified in an area, vessel, or facility security assessment or by the operator that require limited access and a higher degree of security protection. The entire facility may be designated the restricted area, as long as the entire facility is provided the appropriate level of security.

Review and approval means the process whereby Coast Guard officials evaluate a plan or proposal to determine if it complies with this subchapter and/or provides an equivalent level of security.

Screening means a reasonable examination of persons, cargo, vehicles, or baggage for the protection of the vessel, its passengers and crew. The purpose of the screening is to secure the vital government interest of protecting vessels, harbors, and waterfront facilities from destruction, loss, or injury from sabotage or other causes of similar nature. Such screening is intended to ensure that dangerous substances and devices, or other items that pose a real danger of violence or a threat to security are not present.

Security sweep means a walkthrough to visually inspect unrestricted areas to identify unattended packages, briefcases, or luggage and determine that all restricted areas are secure.

Security system means a device or multiple devices designed, installed and operated to monitor, detect, observe or communicate about activity that may pose a security threat in a location or locations on a vessel or facility.

Sensitive security information (SSI) means information within the scope of 49 CFR part 1520.

SOLAS means the International Convention for the Safety of Life at Sea

Convention, 1974, as amended.

Survey means an on-scene examination and evaluation of the physical characteristics of a vessel or facility, and its security systems, processes, procedures, and personnel.

Transportation security incident (TSI) means a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.

Unaccompanied baggage means any baggage, including personal effects, that is not being brought on board on behalf of a person who is boarding the vessel.

Vessel-to-facility interface means the interaction that occurs when a vessel is directly and immediately affected by actions involving the movement of persons, cargo, vessel stores, or the provisions of facility services to or from the vessel.

Vessel-to-port interface means the interaction that occurs when a vessel is directly and immediately affected by actions involving the movement of persons, cargo, vessel stores, or the provisions of port services to or from the vessel.

Vessel Security Assessment (VSA) means an analysis that examines and evaluates the vessel and its operations taking into account possible threats, vulnerabilities, consequences, and existing protective measures, procedures and operations.

Vessel Security Plan (VSP) means the plan developed to ensure the application of security measures designed to protect the vessel and the facility that the vessel is servicing or interacting with, the vessel's cargoes, and persons on board at the respective MARSEC Levels.

Vessel Security Officer (VSO) means the person onboard the vessel, accountable to the Master, designated by the Company as responsible for security of the vessel, including implementation and maintenance of the Vessel Security Plan, and for liaison with the Facility Security Officer and the vessel's Company Security Officer.

Vessel stores means—

(1) Materials that are on board a vessel for the upkeep, maintenance,

safety, operation or navigation of the vessel; and

(2) Materials for the safety or comfort of the vessel's passengers or crew, including any provisions for the vessel's passengers or crew.

Vessel-to-vessel activity means any activity not related to a facility or port that involves the transfer of cargo, vessel stores, or persons from one vessel to another.

Waters subject to the jurisdiction of the U.S., for purposes of this subchapter, includes all waters described in section 2.36(a) of this chapter; the Exclusive Economic Zone, in respect to the living and non-living resources therein; and, in respect to facilities located on the Outer Continental Shelf of the U.S., the waters superjacent thereto.

§ 101.110 Applicability.

Unless otherwise specified, this subchapter applies to vessels, structures, and facilities of any kind, located under, in, on, or adjacent to waters subject to the jurisdiction of the U.S.

§ 101.115 Incorporation by reference.

(a) Certain material is incorporated by reference into this subchapter with the approval of the Director of the Federal Register under 5 U.S.C. 552(a) and 1 CFR part 51. To enforce any edition other than that specified in paragraph (b) of this section, the Coast Guard must publish notice of change in the Federal Register and the material must be available to the public. All approved material is on file at the Office of the Federal Register, 800 North Capitol Street, NW., Suite 700, Washington, DC, and at the Office of the Coast Guard Port Security Directorate (G-MP), Coast Guard Headquarters, 2100 Second Street, SW., Washington, DC 20593-0001, and is available from the sources indicated in paragraph (b) of this section.

(b) The materials approved for incorporation by reference in this subchapter are as follows:

International Maritime Organization (IMO)

Publication Section, 4 Albert Embankment, London SE1 7SR, United Kingdom.

Conference resolution 1, Adoption of amendments to the Annex to the International Convention for the Safety of Life at Sea, 1974, and amendments to Chapter XI of SOLAS 1974, adopted December 12, 2002, (SOLAS Chapter XI-1 or SOLAS Chapter XI-2).

101.120; 101.310; 101.410;
101.505; 104.105; 104.115;
104.120; 104.297; 104.400.

Conference resolution 2, Adoption of the International Code for the Security of Ships and of Port Facilities, parts A and B, adopted on December 12, 2002 (ISPS Code).

101.410; 101.505; 104.105;
104.115; 104.120; 104.297;
104.400.

§ 101.120 Alternatives.

(a) *Alternative Security Agreements.* (1) The U.S. may conclude in writing, as provided in SOLAS Chapter XI-2, Regulation 11 (Incorporated by reference, see §101.115), a bilateral or multilateral agreements with other Contracting Governments to SOLAS on Alternative Security Arrangements covering short international voyages on fixed routes between facilities subject to the jurisdiction of the U.S. and facilities in the territories of those Contracting Governments.

(2) As further provided in SOLAS Chapter XI-2, Regulation 11, a vessel covered by such an agreement shall not conduct any vessel-to-vessel activity with any vessel not covered by the agreement.

(b) *Alternative Security Programs.* (1) Owners and operators of vessels and facilities required to have security plans under part 104, 105, or 106 of this subchapter, other than vessels that are subject to SOLAS Chapter XI, may meet an Alternative Security Program that has been reviewed and approved by the Commandant (G-MP) as meeting the requirements of part 104, 105, or 106,

as applicable.

(2) Owners or operators must implement an approved Alternative Security Program in its entirety to be deemed in compliance with either part 104, 105, or 106.

(3) Owners or operators who have implemented an Alternative Security Program must send a letter to the appropriate plan approval authority under part 104, 105, or 106 of this subchapter identifying which Alternative Security Program they have implemented, identifying those vessels or facilities that will implement the Alternative Security Program, and attesting that they are in full compliance therewith. A copy of this letter shall be retained on board the vessel or kept at the facility to which it pertains along with a copy of the Alternative Security Program and a vessel, facility, or Outer Continental Shelf facility specific security assessment report generated under the Alternative Security Program.

(4) Owners or operators shall make available to the Coast Guard, upon request, any information related to implementation of an approved Alternative Security Program.

(c) *Approval of Alternative Security Programs.* You must submit to the Commandant (G-MP) for review and approval the Alternative Security Program and the following information to assess the adequacy of the proposed Alternative Security Program:

(1) A list of the vessel and facility type that the Alternative Security Program is intended to apply;

(2) A security assessment for the vessel or facility type;

(3) Explanation of how the Alternative Security Program addresses the requirements of parts 104, 105, or 106, as applicable; and

(4) Explanation of how owners and operators must implement the Alternative Security Program in its entirety, including performing an operational and vessel or facility specific assessment and verification of implementation.

(d) *Amendment of Approved Alternative Security Programs.* (1) Amendments to an Alternative Security Program approved under this section may be initiated by—

(i) The submitter of an Alternative Security Program under paragraph (c) of this section; or

(ii) The Coast Guard upon a determination that an amendment is needed to maintain the security of a vessel or facility. The Coast Guard will give the submitter of an Alternative Security Program written notice and request that the submitter propose amendments addressing any matters specified in the notice. The submitter will have at least 60 days to submit its proposed amendments.

(2) Proposed amendments must be sent to the Commandant (G-MP). If initiated by the submitter, the proposed amendment must be submitted at least 30 days before the amendment is to take effect unless the Commandant (G-MP) allows a shorter period. The Commandant (G-MP) will approve or disapprove the proposed amendment in accordance with paragraph (f) of this section.

(e) *Validity of Alternative Security Program.* An Alternative Security Program approved under this section is valid for 5 years from the date of its approval.

(f) The Commandant (G-MP) will examine each submission for compliance with this part, and either:

(1) Approve it and specify any conditions of approval, returning to the submitter a letter stating its acceptance and any conditions;

(2) Return it for revision, returning a copy to the submitter with brief descriptions of the required revisions; or

(3) Disapprove it, returning a copy to the submitter with a brief statement of the reasons for disapproval.

§ 101.125 Approved Alternative Security Programs.

The following have been approved, by the Commandant (G-MP), as Alternative Security Programs, which may be used by vessel or facility owners or operators to meet the provisions of parts 104, 105, or 106 of this subchapter, as applicable:

(a) American Gaming Association Alternative Security

Program, dated September 11, 2003.

(b) American Waterways Operators Alternative Security Program for Tugboats, and Towboats and Barges, dated September 24, 2003.

(c) Passenger Vessel Association Industry Standards for Security of Passenger Vessels and Small Passenger Vessels, dated September 17, 2003.

§ 101.130 Equivalent security measures.

(a) For any measure required by part 104, 105, or 106 of this subchapter, the owner or operator may substitute an equivalent security measure that has been approved by the Commandant (G-MP) as meeting or exceeding the effectiveness of the required measure. The Commandant (G-MP) may require that the owner or operator provide data for use in assessing the effectiveness of the proposed equivalent security measure.

(b) Requests for approval of equivalent security measures should be made to the appropriate plan approval authority under parts 104, 105 or 106 of this subchapter.

Subpart B—Maritime Security (MARSEC) Levels

§ 101.200 MARSEC Levels.

(a) MARSEC Levels advise the maritime community and the public of the level of risk to the maritime elements of the national transportation system. Ports, under direction of the local COTP, will respond to changes in the MARSEC Level by implementing the measures specified in the AMS Plan. Similarly, vessels and facilities required to have security plans under part 104, 105, or 106 of this subchapter shall implement the measures specified in their security plans for the applicable MARSEC Level.

(b) Unless otherwise directed, each port, vessel, and facility shall operate at MARSEC Level 1.

(c) The Commandant will set the MARSEC Level consistent with the equivalent Homeland Security Advisory System (HSAS) Threat

Condition and that Threat Condition's scope of application. Notwithstanding the HSAS, the Commandant retains discretion to adjust the MARSEC Level when necessary to address any particular security concerns or circumstances related to the maritime elements of the national transportation system.

(d) The COTP may temporarily raise the MARSEC Level for the port, a specific marine operation within the port, or a specific industry within the port, when necessary to address an exigent circumstance immediately affecting the security of the maritime elements of the transportation system in his/her area of responsibility.

§ 101.205 Department of Homeland Security alignment.

The MARSEC Levels are aligned with the Department of Homeland Security's Homeland Security Advisory System (HSAS), established by Homeland Security Presidential Directive 3. Table 101.205, titled "Relation between HSAS and MARSEC Levels" in this section, shows this alignment.

Table 101.205 Relation Between Homeland Security Advisory System (HSAS) and Maritime Security (MARSEC) Levels

MARSEC Level 1

HSAS Low: Green
HSAS Guarded: Blue
HSAS Elevated: Yellow

MARSEC Level 2
HSAS High: Orange

MARSEC Level 3
HSAS Severe: Red

**Subpart C—Communication
(Port—Facility—Vessel)**

§ 101.300 Preparedness communications.

(a) *Notification of MARSEC Level change.* The COTP will

communicate any changes in the MARSEC Levels through a local Broadcast Notice to Mariners, an electronic means, if available, or as detailed in the AMS Plan.

(b) *Communication of threats.*

When the COTP is made aware of a threat that may cause a transportation security incident, the COTP will, when appropriate, communicate to the port stakeholders, vessels, and facilities in his or her AOR the following details:

(1) Geographic area potentially impacted by the probable threat;

(2) Any appropriate information identifying potential targets;

(3) Onset and expected duration of probable threat;

(4) Type of probable threat; and

(5) Required actions to minimize risk.

(c) *Attainment.* (1) Each owner or operator of a vessel or facility required to have a security plan under parts 104 or 105 of this subchapter affected by a change in the MARSEC Level must ensure confirmation to their local COTP the attainment of measures or actions described in their security plan and any other requirements imposed by the COTP that correspond with the MARSEC Level being imposed by the change.

(2) Each owner or operator of a facility required to have a security plan under part 106 of this subchapter affected by a change in the MARSEC Level must must confirm to their cognizant District Commander the attainment of measures or actions described in their security plan and any other requirements imposed by the District Commander or COTP that correspond with the MARSEC Level being imposed by the change.

§ 101.305 Reporting.

(a) *Notification of suspicious activities.* An owner or operator required to have a security plan under part 104, 105, or 106 of this subchapter shall, without delay, report activities that may result in a transportation security incident to the National Response Center at the following toll free telephone: 1-800-424-8802, direct telephone: 202-267-2675, fax:

202–267–2165, TDD: 202–267–4477, or Email: *lst-nrcinfo@comdt.uscg.mil*.

Any other person or entity is also encouraged to report activities that may result in a transportation security incident to the National Response Center.

(b) *Notification of breaches of security.* An owner or operator required to have a security plan under parts 104, 105, or 106 of this subchapter shall, without delay, report breaches of security to the National Response Center via one of the means listed in paragraph (a) of this section.

(c) *Notification of transportation security incident (TSI).* (1) Any owner or operator required to have a security plan under part 104 or 105 of this subchapter shall, without delay, report a TSI to their local COTP and immediately thereafter begin following the procedures set out in their security plan, which may include contacting the National Response Center via one of the means listed in paragraph (a) of this section.

(2) Any owner or operator required to have a security plan under part 106 of this subchapter shall, without delay, report a TSI to their cognizant District Commander and immediately thereafter begin following the procedures set out in their security plan, which may include contacting the National Response Center via one of the means listed in paragraph (a) of this section.

(d) Callers to the National Response Center should be prepared to provide as much of the following information as possible:

(1) Their own name and contact information;

(2) The name and contact information of the suspicious or responsible party;

(3) The location of the incident, as specifically as possible; and

(4) The description of the incident or activity involved.

§ 101.310 Additional communication devices.

(a) *Alert Systems.* Alert systems, such as the ship security alert system required in SOLAS Chapter XI–2,

Regulation 6 (Incorporated by reference, see §101.115), may be used to augment communication and may be one of the communication methods listed in a vessel or facility security plan under part 104, 105, or 106 of this subchapter.

(b) *Automated Identification Systems (AIS).* AIS may be used to augment communication, and may be one of the communication methods listed in a vessel security plan under part 104 of this subchapter. See 33 CFR part 164 for additional information on AIS device requirements.

Subpart D—Control Measures for Security

§ 101.400 Enforcement.

(a) The rules and regulations in this subchapter are enforced by the COTP under the supervision and general direction of the District Commander, Area Commander, and the Commandant. All authority and power vested in the COTP by the rules and regulations in this subchapter is also vested in, and may be exercised by, the District Commander, Area Commander, and the Commandant.

(b) The COTP, District Commander, Area Commander, or Commandant may assign the enforcement authority described in paragraph (a) of this section to any other officer or petty officer of the Coast Guard or other designees authorized by the Commandant.

(c) The provisions in this subchapter do not limit the powers conferred upon Coast Guard commissioned, warrant, or petty officers by any other law or regulation, including but not limited to 33 CFR parts 6, 160, and 165.

§ 101.405 Maritime Security (MARSEC) Directives.

(a)(1) When the Coast Guard determines that additional security measures are necessary to respond to a threat assessment or to a specific threat against the maritime elements of the national transportation system, the Coast Guard may issue a MARSEC Directive setting forth mandatory

measures. Only the Commandant or his/her delegatee may issue MARSEC Directives under this section. Prior to issuing a MARSEC Directive, the Commandant or his/her delegatee will consult with those Federal agencies having an interest in the subject matter of that MARSEC Directive. All MARSEC Directives issued under this section shall be marked as sensitive security information (SSI) in accordance with 49 CFR part 1520.

(2) When a MARSEC Directive is issued, the Coast Guard will immediately publish a notice in the Federal Register, and affected owners and operators will need to go to their local COTP or cognizant District Commander to acquire a copy of the MARSEC Directive. COTPs and District Commanders will require owners or operators to prove that they are a person required by 49 CFR 1520.5(a) to restrict disclosure of and access to sensitive security information, and that under 49 CFR 1520.5(b), they have a need to know sensitive security information.

(b) Each owner or operator of a vessel or facility to whom a MARSEC Directive applies is required to comply with the relevant instructions contained in a MARSEC Directive issued under this section within the time prescribed by that MARSEC Directive.

(c) Each owner or operator of a vessel or facility required to have a security plan under parts 104, 105 or 106 of this subchapter that receives a MARSEC Directive must:

(1) Within the time prescribed in the MARSEC Directive, acknowledge receipt of the MARSEC Directive to their local COTP or, if a facility regulated under part 106 of this subchapter, to their cognizant District Commander; and

(2) Within the time prescribed in the MARSEC Directive, specify the method by which the measures in the MARSEC Directive have been implemented (or will be implemented, if the MARSEC Directive is not yet effective).

(d) In the event that the owner or operator of a vessel or facility required to have a security plan under part 104, 105, or 106 of this subchapter

is unable to implement the measures in the MARSEC Directive, the owner or operator must submit proposed equivalent security measures and the basis for submitting the equivalent security measures to the COTP or, if a facility regulated under part 106 of this subchapter, to their cognizant District Commander, for approval.

(e) The owner or operator must submit the proposed equivalent security measures within the time prescribed in the MARSEC Directive. The owner or operator must implement any equivalent security measures approved by the COTP, or, if a facility regulated under part 106 of this subchapter, by their cognizant District Commander.

§ 101.410 Control and Compliance Measures.

(a) The COTP may exercise authority pursuant to 33 CFR parts 6, 160 and 165, as appropriate, to rectify non-compliance with this subchapter. COTPs or their designees are the officers duly authorized to exercise control and compliance measures under SOLAS Chapter XI-2, Regulation 9, and the ISPS Code (Incorporated by reference, see §101.115).

(b) Control and compliance measures for vessels not in compliance with this subchapter may include, but are not limited to, one or more of the following:

- (1) Inspection of the vessel;
- (2) Delay of the vessel;
- (3) Detention of the vessel;
- (4) Restriction of vessel operations;

- (5) Denial of port entry;
- (6) Expulsion from port;
- (7) Lesser administrative and corrective measures; or

(8) Suspension or revocation of a security plan approved by the U.S., thereby making that vessel ineligible to operate in, on, or under waters subject to the jurisdiction of the U.S. in accordance with 46 U.S.C. 70103(c)(5).

(c) Control and compliance measures for facilities not in compliance with this subchapter may include, but are not limited to, one or more of the following:

- (1) Restrictions on facility

access;

(2) Conditions on facility operations;

(3) Suspension of facility operations;

(4) Lesser administrative and corrective measures; or

(5) Suspension or revocation of security plan approval, thereby making that facility ineligible to operate in, on, under or adjacent to waters subject to the jurisdiction of the U.S. in accordance with 46 U.S.C. 70103(c)(5).

(d) Control and compliance measures under this section may be imposed on a vessel when it has called on a facility or at a port that does not maintain adequate security measures to ensure that the level of security to be achieved by this subchapter has not been compromised.

§ 101.415 Penalties.

(a) *Civil and criminal penalty.* Violation of any order or other requirement imposed under section 101.405 of this part is punishable by the civil and criminal penalties prescribed in 33 U.S.C. 1232 or 50 U.S.C. 192, as appropriate.

(b) *Civil penalty.* As provided in 46 U.S.C. 70117, any person who does not comply with any other applicable requirement under this subchapter, including a Maritime Security Directive, shall be liable to the U.S. for a civil penalty of not more than \$25,000 for each violation. Enforcement and administration of this provision will be in accordance with 33 CFR 1.07.

§ 101.420 Right to appeal.

(a) Any person directly affected by a decision or action taken by a COTP under this subchapter, may appeal that action or decision to the cognizant District Commander according to the procedures in 46 CFR 1.03–15.

(b) Any person directly affected by a decision or action taken by a District Commander, whether made under this subchapter generally or pursuant to paragraph (a) of this section, with the exception of those decisions made under § 101.410 of this subpart, may appeal that decision or action to the Commandant (G-MP), according to

the procedures in 46 CFR 1.03-15. Appeals of District Commander decisions or actions made under § 101.410 of this subpart should be made to the Commandant (G-MOC), according to the procedures in 46 CFR 1.03-15.

(c) Any person directly affected by a decision or action taken by the Commanding Officer, Marine Safety Center, under this subchapter, may appeal that action or decision to the Commandant (G-MP) according to the procedures in 46 CFR 1.03–15.

(d) Decisions made by Commandant (G-MP), whether made under this subchapter generally or pursuant to the appeal provisions of this section, are considered final agency action.

Subpart E—Other Provisions

§ 101.500 Procedures for authorizing a Recognized Security Organization (RSO). [Reserved]

§ 101.505 Declaration of Security (DoS).

(a) The purpose of a DoS, as described in SOLAS Chapter XI–2, Regulation 10, and the ISPS Code (Incorporated by reference, see §101.115), is to state the agreement reached between a vessel and a facility, or between vessels in the case of a vessel-to-vessel activity, as to the respective security measures each must undertake during a specific vessel-to-facility interface, during a series of interfaces between the vessel and the facility, or during a vessel-to-vessel activity.

(b) Details as to who must complete a DoS, when a DoS must be completed, and how long a DoS must be retained are included in parts 104 through 106 of this subchapter. A DoS must, at a minimum, include the information found in the ISPS Code, part B, appendix 1 (Incorporated by reference, see § 101.115).

(c) All vessels and facilities required to comply with parts 104, 105, and 106 of this subchapter must, at a minimum, comply with the DoS requirements of the MARSEC Level set

for the port.

(d) The COTP may also require a DoS be completed for vessels and facilities during periods of critical port operations, special marine events, or when vessels give notification of a higher MARSEC Level than that set in the COTP's Area of Responsibility (AOR).

§ 101.510 Assessment tools.

Ports, vessels, and facilities required to conduct security assessments by part 103, 104, 105, or 106 of this subchapter may use any assessment tool that meets the standards set out in part 103, 104, 105, or 106, as applicable. These tools may include:

(a) DHS/TSA's vulnerability self-assessment tool located at <http://www.tsa.gov/risk>; and

(b) USCG assessment tools, available from the cognizant COTP or at <http://www.uscg.mil/hq/g-m/nvic>, as set out in the following:

(1) Navigation and Vessel Inspection Circular titled, "Guidelines for Port Security Committees, and Port Security Plans Required for U.S. Ports" (NVIC 9-02);

(2) Navigation and Vessel Inspection Circular titled, "Security Guidelines for Vessels", (NVIC 10-02); and

(3) Navigation and Vessel Inspection Circular titled, "Security Guidelines for Facilities", (NVIC 11-02).

§ 101.515 Personal identification.

(a) Any personal identification credential accepted under the access control provisions of this subchapter must, at a minimum, meet the following requirements:

(1) Be laminated or otherwise secure against tampering;

(2) Contain the individual's full name (full first and last names, middle initial is acceptable);

(3) Contain a photo that accurately depicts that individual's current facial appearance; and

(4) Bear the name of the issuing authority.

(b) The issuing authority in paragraph (a)(4) of this section must be:

(1) A government authority, or an organization authorized to act on behalf of a government authority; or

(2) The individual's employer, union, or trade association.

(c) Vessel, facility, and OCS facility owners and operators must permit law enforcement officials, in the performance of their official duties, who present proper identification in accordance with this section to enter or board that vessel, facility, or OCS facility at any time, without delay or obstruction. Law enforcement officials, upon entering or boarding a vessel, facility, or OCS facility, will, as soon as practicable, explain their mission to the Master, owner, or operator, or their designated agent.

33 CFR
Navigation and Navigable Waters
CHAPTER I
COAST GUARD, DEPARTMENT
OF HOMELAND SECURITY
SUBCHAPTER H — MARITIME
SECURITY

PART 103—MARITIME
SECURITY: AREA MARITIME
SECURITY

Subpart A — General

Sec.

- 103.100 Applicability.
 103.105 Definitions.

Subpart B — Federal Maritime
Security Coordinator (FMSC)
Designation and Authorities

- 103.200 Designation of the Federal Maritime Security Coordinator (FMSC).
 103.205 Authority of the COTP as the Federal Maritime Security Coordinator (FMSC).

Subpart C — Area Maritime
Security (AMS) Committee

- 103.300 Area Maritime Security (AMS) Committee.
 103.305 Composition of an Area Maritime Security (AMS) Committee.
 103.310 Responsibilities of the Area Maritime Security (AMS) Committee.

Subpart D — Area Maritime
Security (AMS) Assessment

- 103.400 General.
 103.405 Elements of the Area Maritime Security (AMS) Assessment.
 103.410 Persons involved in the Area Maritime Security (AMS) Assessment.

Subpart E — Area Maritime
Security (AMS) Plan

- 103.500 General.
 103.505 Elements of the Area Maritime Security (AMS) Plan.
 103.510 Area Maritime Security (AMS) Plan review and approval.
 103.515 Exercises.
 103.520 Recordkeeping.

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. 70102, 70103, 70104, 70112; 50 U.S.C. 191; 33 CFR 1.05–1, 6.04–11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No. 0170.1.

Source: USCG-2003-14733, 68 FR 39290, July 1, 2003, unless otherwise noted.

Subpart A—General

§ 103.100 Applicability.

This part applies to all vessels and facilities located in, on, under, or adjacent to waters subject to the jurisdiction of the U.S.

§ 103.105 Definitions.

Except as specifically stated in this subpart, the definitions in part 101 of this subchapter apply to this part.

Subpart B—Federal Maritime
Security Coordinator (FMSC)
Designation and Authorities

§ 103.200 Designation of the
Federal Maritime Security Coordi-
nator (FMSC).

The COTPs are the Federal Maritime Security Coordinators for their respective COTP zones described in 33 CFR part 3, including all ports and areas located therein.

§ 103.205 Authority of the COTP
as the Federal Maritime Security
Coordinator (FMSC).

(a) Without limitation to the authority vested in the COTP by statute or regulation, and in addition to authority prescribed elsewhere in this part, the COTP as the FMSC is authorized to:

- (1) Establish, convene, and direct the Area Maritime Security (AMS) Committee;
 - (2) Appoint members to the AMS Committee;
 - (3) Develop and maintain, in coordination with the AMS Committee, the AMS Plan;
 - (4) Implement and exercise the AMS Plan; and
 - (5) Maintain the records required by §103.520 of this part.
- (b) The authorizations in para-

graph (a) of this section do not limit any other existing authority of the COTP.

Subpart C—Area Maritime Security (AMS) Committee

§ 103.300 Area Maritime Security (AMS) Committee.

(a) The AMS Committee is established under the direction of the COTP and shall assist in the development, review, and update of the AMS Plan for their area of responsibility. For the purposes of this subchapter, Port Security Committees that were established prior to July 1, 2003, according to guidance issued by the Coast Guard, may be considered AMS Committees, provided they conform to the procedures established by this part and satisfy the membership requirements of § 103.305 of this part.

(b) The AMS Committee will operate under terms specified in a written charter. At a minimum, the charter must address:

- (1) The AMS Committee's purpose and geographic area of responsibility;
- (2) Rules for membership;
- (3) The AMS Committee's organizational structure and procedural rules of order;
- (4) Frequency of meetings, to include not less than once in a calendar year or when requested by a majority of the AMS Committee members;
- (5) Guidelines for public access to AMS Committee meetings and records; and
- (6) Rules for handling and protecting classified, sensitive security, commercially sensitive, and proprietary information.

§ 103.305 Composition of an Area Maritime Security (AMS) Committee.

(a) An AMS Committee will be composed of not less than seven members having an interest in the security of the area and who may be selected from—

- (1) The Federal, Territorial, or Tribal government;
- (2) The State government and political subdivisions thereof;

(3) Local public safety, crisis management and emergency response agencies;

(4) Law enforcement and security organizations;

(5) Maritime industry, including labor;

(6) Other port stakeholders having a special competence in maritime security; and

(7) Port stakeholders affected by security practices and policies.

(b) At least seven of the members must each have 5 or more years of experience related to maritime or port security operations.

(c) Members appointed under this section serve for a term of not more than 5 years. In appointing members, the COTP should consider the skills required by § 103.410 of this part. Prior to the appointment of an individual to a position on the AMS Committee, the COTP may require an appropriate security background examination of the candidate member.

§ 103.310 Responsibilities of the Area Maritime Security (AMS) Committee.

(a) The AMS Committee shall:

- (1) Identify critical port infrastructure and operations;
- (2) Identify risks (threats, vulnerabilities, and consequences);
- (3) Determine mitigation strategies and implementation methods;
- (4) Develop and describe the process to continually evaluate overall port security by considering consequences and vulnerabilities, how they may change over time, and what additional mitigation strategies can be applied; and
- (5) Provide advice to, and assist the COTP in, developing the AMS Plan.

(b) The AMS Committee shall also serve as a link for communicating threats and changes in MARSEC Levels, and disseminating appropriate security information to port stakeholders.

Subpart D—Area Maritime Security (AMS) Assessment

§ 103.400 General.

(a) The Area Maritime Security (AMS) Committee will ensure that a

risk based AMS Assessment, is completed and meets the requirements specified in §103.310 of this part and §101.510 of this subchapter, incorporating the elements specified in §103.405 of this part.

(b) AMS Assessments can be completed by the COTP, the AMS Committee, a Coast Guard Port Security Assessment team, or by another third party approved by the AMS Committee.

(c) Upon completion of each AMS Assessment, a written report, which is designated sensitive security information, must be prepared consisting of:

- (1) A summary of how the AMS Assessment was conducted;
- (2) A description of each vulnerability and consequences found during the AMS Assessment; and
- (3) A description of risk reduction strategies that could be used to ensure continued operation at an acceptable risk level.

§ 103.405 Elements of the Area Maritime Security (AMS) Assessment.

(a) The AMS Assessment must include the following elements:

- (1) Identification of the critical Marine Transportation System infrastructure and operations in the port;
 - (2) Threat assessment that identifies and evaluates each potential threat on the basis of various factors, including capability and intention;
 - (3) Consequence and vulnerability assessment for each target/scenario combination; and
 - (4) A determination of the required security measures for the three MARSEC Levels.
- (b) In order to meet the elements listed in paragraph (a) of this section, an AMS Assessment should consider each of the following:
- (1) Physical security of infrastructure and operations at the port;
 - (2) Structures considered critical for the continued operation of the port;
 - (3) Existing security systems and equipment available to protect maritime personnel;
 - (4) Procedural policies;
 - (5) Radio and telecommunica-

tion systems, including computer systems and networks;

- (6) Relevant transportation infrastructure;
- (7) Utilities;
- (8) Security resources and capabilities; and
- (9) Other areas that may, if damaged, pose a risk to people, infrastructure, or operations within the port.

(c) AMS Assessments are sensitive security information and must be protected in accordance with 49 CFR part 1520.

§ 103.410 Persons involved in the Area Maritime Security (AMS) Assessment.

The persons carrying out the AMS Assessment must have the appropriate skills to evaluate the security of the port in accordance with this part. This includes being able to draw upon expert assistance in relation to:

- (a) Knowledge of current security threats and patterns;
- (b) Recognition and detection of dangerous substances, and devices;
- (c) Recognition, on a non-discriminatory basis, of characteristics and behavioral patterns of persons who are likely to threaten security;
- (d) Techniques used to circumvent security measures;
- (e) Methods used to cause a transportation security incident;
- (f) Effects of dangerous substances and devices on structures and port services;
- (g) Port security requirements;
- (h) Port business practices;
- (i) Contingency planning, emergency preparedness, and response;
- (j) Physical security measures;
- (k) Radio and telecommunications systems, including computer systems and networks;
- (l) Transportation and civil engineering;
- (m) Vessel and port operations; and
- (n) Knowledge of the impact, including cost impacts of implementing security measures on port operations.

Subpart E—Area Maritime

Security (AMS) Plan**§ 103.500 General.**

(a) The Area Maritime Security (AMS) Plan is developed by the COTP, in consultation with the AMS Committee, and is based on an AMS Assessment that meets the provisions of subpart D of this part. The AMS Plan must be consistent with the National Maritime Transportation Security Plan and the National Transportation Security Plan.

(b) Portions of the AMS Plan may contain sensitive security information, and those portions must be marked as such and protected in accordance with 49 CFR part 1520.

§ 103.505 Elements of the Area Maritime Security (AMS) Plan.

The AMS Plan should address the following elements, as applicable:

(a) Details of both operational and physical measures that are in place in the port at MARSEC Level 1;

(b) Details of the additional security measures that enable the port to progress, without delay, to MARSEC Level 2 and, when necessary, to MARSEC Level 3;

(c) Details of the security incident command-and-response structure;

(d) Details for regular audit of the AMS Plan, and for its amendment in response to experience or changing circumstances;

(e) Measures to prevent the introduction of dangerous substances and devices into designated restricted areas within the port;

(f) Measures to prevent unauthorized access to designated restricted areas within the port;

(g) Procedures and expected timeframes for responding to security threats or breaches of security, including provisions for maintaining infrastructure and operations in the port;

(h) Procedures for responding to any security instructions the Coast Guard announces at MARSEC Level 3;

(i) Procedures for evacuation within the port in case of security threats or breaches of security;

(j) Procedures for periodic plan review, exercise, and updating;

(k) Procedures for reporting transportation security incidents (TSI);

(l) Identification of, and methods to communicate with, Facility Security Officers (FSO), Company Security Officers (CSO), Vessel Security Officers (VSO), public safety officers, emergency response personnel, and crisis management organization representatives within the port, including 24-hour contact details;

(m) Measures to ensure the security of the information contained in the AMS Plan;

(n) Security measures designed to ensure effective security of infrastructure, special events, vessels, passengers, cargo, and cargo handling equipment at facilities within the port not otherwise covered by a Vessel or Facility Security Plan, approved under part 104, 105, or 106 of this subchapter;

(o) Procedures to be taken when a vessel is at a higher security level than the facility or port it is visiting;

(p) Procedures for responding if a vessel security alert system on board a vessel within or near the port has been activated;

(q) Procedures for communicating appropriate security and threat information to the public;

(r) Procedures for handling reports from the public and maritime industry regarding suspicious activity;

(s) The jurisdiction of Federal, State, Indian Tribal, and local government agencies and law enforcement entities over area security related matters;

(t) Security resources available for incident response and their capabilities;

(u) Procedures for responding to a TSI;

(v) Procedures to facilitate the recovery of the Marine Transportation System after a TSI; and

(w) Identification of any facility otherwise subject to part 105 of this subchapter that the COTP has designated as a public access facility within the area, the security measures that must be implemented at the various MARSEC Levels, and who is responsible for implementing those measures.

§ 103.510 Area Maritime Security (AMS) Plan review and approval.

Each AMS Plan will be submitted to the cognizant District Commander for review and then forwarded to the Area Commander for approval.

§ 103.515 Exercises.

(a) The COTP shall coordinate with the Area Maritime Security (AMS) Committee to conduct or participate in an exercise at least once each calendar year, with no more than 18 months between exercises, to test the effectiveness of the AMS Plan.

(b) An exercise may consist of any of the following:

(1) A tabletop exercise to validate the AMS Plan. No equipment or personnel deployment is required;

(2) A field training exercise consisting of personnel deployment and use of security equipment; or

(3) A combination of §103.515(b)(1) and (b)(2).

(c) Upon review by the cognizant District Commander, and

approval by the cognizant Area Commander, the requirements of this section may be satisfied by—

(1) Participation of the COTP and appropriate AMS Committee members or other appropriate port stakeholders in an emergency response or crisis management exercise conducted by another governmental agency or private sector entity, provided that the exercise addresses components of the AMS Plan;

(2) An actual increase in MARSEC Level; or

(3) Implementation of enhanced security measures enumerated in the AMS Plan during periods of critical port operations or special marine events.

§ 103.520 Recordkeeping.

(a) All records pertaining to the Area Maritime Security (AMS) Assessment and AMS Plan will be retained by the COTP for 5 years.

(b) Exercise documentation will be kept by the COTP for 2 years.

33 CFR
Navigation and Navigable Waters
CHAPTER I
COAST GUARD, DEPARTMENT
OF HOMELAND SECURITY
SUBCHAPTER H -- MARITIME
SECURITY

PART 104—MARITIME
SECURITY: VESSELS

Subpart A -- General

Sec.

- 104.100 Definitions.
- 104.105 Applicability.
- 104.110 Exemptions.
- 104.115 Compliance dates.
- 104.120 Compliance documentation.
- 104.125 Noncompliance.
- 104.130 Waivers.
- 104.135 Equivalents.
- 104.140 Alternative Security Programs.
- 104.145 Maritime Security (MARSEC) Directive.
- 104.150 Right to appeal.

Subpart B -- Vessel Security Requirements

- 104.200 Owner or operator.
- 104.205 Master.
- 104.210 Company Security Officer (CSO).
- 104.215 Vessel Security Officer (VSO).
- 104.220 Company or vessel personnel with security duties.
- 104.225 Security training for all other vessel personnel.
- 104.230 Drill and exercise requirements.
- 104.235 Vessel recordkeeping requirements.
- 104.240 Maritime Security (MARSEC) Level coordination and implementation.
- 104.245 Communications.
- 104.250 Procedures for interfacing with facilities and other vessels.
- 104.255 Declaration of Security (DoS).
- 104.260 Security systems and equipment maintenance.
- 104.265 Security measures for

access control.

- 104.270 Security measures for restricted areas.
- 104.275 Security measures for handling cargo.
- 104.280 Security measures for delivery of vessel stores and bunkers.
- 104.285 Security measures for monitoring.
- 104.290 Security incident procedures.
- 104.292 Additional requirements—passenger vessels and ferries.
- 104.295 Additional requirements—cruise ships.
- 104.297 Additional requirements—vessels on international voyages.

Subpart C -- Vessel Security Assessment (VSA)

- 104.300 General.
- 104.305 Vessel Security Assessment (VSA) requirements.
- 104.310 Submission requirements.

Subpart D -- Vessel Security Plan (VSP)

- 104.400 General.
- 104.405 Format of the Vessel Security Plan (VSP).
- 104.410 Submission and approval.
- 104.415 Amendment and audit.

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. Chapter 701; 50 U.S.C. 191; 33 CFR 1.05–1, 6.04–11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No. 0170.1.

Source: USCG-2003-14749, 68 FR 39302, July 1, 2003, unless otherwise noted.

Subpart A—General

§ 104.100 Definitions.

Except as specifically stated in this subpart, the definitions in part 101 of this subchapter apply to this part.

§ 104.105 Applicability.

(a) This part applies to the owner or operator of any:

(1) Mobile Offshore Drilling Unit (MODU), cargo, or passenger vessel subject to the International Convention for Safety of Life at Sea,

1974, (SOLAS), Chapter XI;

(2) Foreign cargo vessel greater than 100 gross register tons;

(3) Self-propelled U.S. cargo vessel greater than 100 gross register tons subject to 46 CFR subchapter I, except commercial fishing vessels inspected under 46 CFR part 105;

(4) Vessel subject to 46 CFR chapter I, subchapter L;

(5) Passenger vessel subject to 46 CFR chapter I, subchapter H;

(6) Passenger vessel certificated to carry more than 150 passengers;

(7) Other passenger vessel carrying more than 12 passengers, including at least one passenger-for-hire, that is engaged on an international voyage;

(8) Barge subject to 46 CFR chapter I, subchapters D or O;

(9) Barge subject to 46 CFR chapter I, subchapter I, that carries Certain Dangerous Cargoes in bulk, or that is engaged on an international voyage;

(10) Tankship subject to 46 CFR chapter I, subchapters D or O; and

(11) Towing vessel greater than eight meters in registered length that is engaged in towing a barge or barges subject to this part, except a towing vessel that--

(i) Temporarily assists another vessel engaged in towing a barge or barges subject to this part;

(ii) Shifts a barge or barges subject to this part at a facility or within a fleeting facility;

(iii) Assists sections of a tow through a lock; or

(iv) Provides emergency assistance.

(b) An owner or operator of any vessel not covered in paragraph (a) of this section is subject to parts 101 through 103 of this subchapter.

(c) Foreign Vessels that have on board a valid International Ship Security Certificate that certifies that the verifications required by part A, Section 19.1, of the International Ship and Port Facility Security (ISPS) Code (Incorporated by reference, see § 101.115 of this subchapter) have been completed will be deemed in compliance with this part, except for §§ 104.240, 104.255, 104.292, and

104.295, as appropriate. This includes ensuring that the vessel meets the applicable requirements of SOLAS Chapter XI-2 (Incorporated by reference, see § 101.115 of this subchapter) and the ISPS Code, part A, having taken into account the relevant provisions of the ISPS Code, part B, and that the vessel is provided with an approved security plan.

(d) Except pursuant to international treaty, convention, or agreement to which the U.S. is a party, this part does not apply to any foreign vessel that is not destined for, or departing from, a port or place subject to the jurisdiction of the U.S. and that is in:

(1) Innocent passage through the territorial sea of the U.S.; or

(2) Transit through the navigable waters of the U.S. that form a part of an international strait.

§ 104.110 Exemptions.

(a) This part does not apply to warships, naval auxiliaries, or other vessels owned or operated by a government and used only on government non-commercial service.

(b) A vessel is not subject to this part while the vessel is laid up, dismantled, or otherwise out of commission.

§ 104.115 Compliance dates.

(a) On July 1, 2004, and thereafter, vessel owners or operators must ensure their vessels are operating in compliance with this part.

(b) On or before December 31, 2003, vessel owners or operators not subject to paragraph (c)(1) of this section must submit to the Commanding Officer, Marine Safety Center, for each vessel—

(1) The Vessel Security Plan described in subpart D of this part for review and approval; or

(2) If intending to operate under an approved Alternative Security Program, a letter signed by the vessel owner or operator stating which approved Alternative Security Program the owner or operator intends to use.

(c) On July 1, 2004, and thereafter, owners or operators of

foreign vessels must comply with the following--

(1) Vessels subject to the International Convention for Safety of Life at Sea, 1974, (SOLAS), Chapter XI, must carry on board a valid International Ship Security Certificate that certifies that the verifications required by part A, Section 19.1, of the International Ship and Port Facility Security (ISPS) Code (Incorporated by reference, see § 101.115 of this subchapter) have been completed. This includes ensuring that the vessel meets the applicable requirements of SOLAS Chapter XI-2 (Incorporated by reference, see § 101.115 of this chapter) and the ISPS Code, part A, having taken into account the relevant provisions of the ISPS Code, part B, and that the vessel is provided with an approved security plan.

(2) Vessels not subject to SOLAS Chapter XI, may comply with this part through an Alternative Security Program or a bilateral arrangement approved by the Coast Guard. If not complying with an approved Alternative Security Program or bilateral arrangement, these vessels must meet the requirements of paragraph (b) of this section.

§ 104.120 Compliance documentation.

(a) Each vessel owner or operator subject to this part must ensure, on or before July 1, 2004, that copies of the following documents are carried on board the vessel and are made available to the Coast Guard upon request:

(1) The approved Vessel Security Plan (VSP) and any approved revisions or amendments thereto, and a letter of approval from the Commanding Officer, Marine Safety Center (MSC);

(2) The VSP submitted for approval and a current acknowledgement letter from the Commanding Officer, MSC, stating that the Coast Guard is currently reviewing the VSP submitted for approval, and that the vessel may continue to operate so long as the vessel remains in compliance with the submitted plan;

(3) For vessels operating under

a Coast Guard-approved Alternative Security Program as provided in §104.140, a copy of the Alternative Security Program the vessel is using, including a vessel specific security assessment report generated under the Alternative Security Program, as specified in § 101.120(b)(3) of this subchapter, and a letter signed by the vessel owner or operator, stating which Alternative Security Program the vessel is using and certifying that the vessel is in full compliance with that program; or

(4) For foreign vessels, subject to the International Convention for Safety of Life at Sea, 1974, (SOLAS), Chapter XI, a valid International Ship Security Certificate (ISSC) that attests to the vessel's compliance with SOLAS Chapter XI-2 and the ISPS Code, part A (Incorporated by reference, see § 101.115 of this subchapter) and is issued in accordance with the ISPS Code, part A, section 19. As stated in Section 9.4 of the ISPS Code, part A requires that, in order for the ISSC to be issued, the provisions of part B of the ISPS Code need to be taken into account.

(b) Each owner or operator of an unmanned vessel subject to this part must maintain the documentation described in paragraphs (a)(1), (2), or (3) of this section. The letter required by each of those paragraphs must be carried on board the vessel. The plan or program required by each of those paragraphs must not be carried on board the vessel, but must be maintained in a secure location. During scheduled inspections, the plan or program must be made available to the Coast Guard upon request.

§ 104.125 Noncompliance.

When a vessel must temporarily deviate from the requirements of this part, the vessel owner or operator must notify the cognizant COTP, and either suspend operations or request and receive permission from the COTP to continue operating.

§ 104.130 Waivers.

Any vessel owner or operator may apply for a waiver of any requirement

of this part that the owner or operator considers unnecessary in light of the nature or operating conditions of the vessel. A request for a waiver must be submitted in writing with justification to the Commandant (G-MP) at 2100 Second St., SW., Washington, DC 20593. The Commandant (G-MP) may require the vessel owner or operator to provide additional data for determining the validity of the requested waiver. The Commandant (G-MP) may grant, in writing, a waiver with or without conditions only if the waiver will not reduce the overall security of the vessel, its passengers, its crew, or its cargo, or facilities or ports that the vessel may visit.

§ 104.135 Equivalents.

For any measure required by this part, the vessel owner or operator may propose an equivalent as provided in §101.130 of this subchapter.

§ 104.140 Alternative Security Programs.

A vessel owner or operator may use an Alternative Security Program as approved under §101.120 of this subchapter if:

- (a) The Alternative Security Program is appropriate to that class of vessel;
- (b) The vessel is not subject to the International Convention for Safety of Life at Sea, 1974; and
- (c) The Alternative Security Program is implemented in its entirety.

§ 104.145 Maritime Security (MARSEC) Directive.

Each vessel owner or operator subject to this part must comply with any instructions contained in a MARSEC Directive issued under §101.405 of this subchapter.

§ 104.150 Right to appeal.

Any person directly affected by a decision or action taken under this part, by or on behalf of the Coast Guard, may appeal as described in §101.420 of this subchapter.

Subpart B—Vessel Security

Requirements

§ 104.200 Owner or operator.

(a) Each vessel owner or operator must ensure that the vessel operates in compliance with the requirements of this part.

(b) For each vessel, the vessel owner or operator must:

(1) Define the security organizational structure for each vessel and provide all personnel exercising security duties or responsibilities within that structure with the support needed to fulfill security obligations;

(2) Designate, in writing, by name or title, a Company Security Officer (CSO), a Vessel Security Officer (VSO) for each vessel, and identify how those officers can be contacted at any time;

(3) Ensure personnel receive training, drills, and exercises enabling them to perform their assigned security duties;

(4) Ensure vessel security records are kept;

(5) Ensure that adequate coordination of security issues takes place between vessels and facilities; this includes the execution of a Declaration of Security (DoS);

(6) Ensure coordination of shore leave for vessel personnel or crew change-out, as well as access through the facility of visitors to the vessel (including representatives of seafarers' welfare and labor organizations), with facility operators in advance of a vessel's arrival. Vessel owners or operators may refer to treaties of friendship, commerce, and navigation between the U.S. and other nations in coordinating such leave. The text of these treaties can be found on the U.S. Department of State's website at <http://www.state.gov/s/l/24224.htm>;

(7) Ensure security communication is readily available;

(8) Ensure coordination with and implementation of changes in Maritime Security (MARSEC) Level;

(9) Ensure that security systems and equipment are installed and maintained;

(10) Ensure that vessel access, including the embarkation of persons

and their effects, are controlled;

(11) Ensure that restricted areas are controlled;

(12) Ensure that cargo and vessel stores and bunkers are handled in compliance with this part;

(13) Ensure restricted areas, deck areas, and areas surrounding the vessel are monitored;

(14) Provide the Master, or for vessels on domestic routes only, the CSO, with the following information:

(i) Parties responsible for appointing vessel personnel, such as vessel management companies, manning agents, contractors, concessionaires (for example, retail sales outlets, casinos, etc.);

(ii) Parties responsible for deciding the employment of the vessel, including time or bareboat charters or any other entity acting in such capacity; and

(iii) In cases when the vessel is employed under the terms of a charter party, the contract details of those documents, including time or voyage charters; and

(15) Give particular consideration to the convenience, comfort, and personal privacy of vessel personnel and their ability to maintain their effectiveness over long periods.

§ 104.205 Master.

(a) Nothing in this part is intended to permit the Master to be constrained by the Company, the vessel owner or operator, or any other person, from taking or executing any decision which, in the professional judgment of the Master, is necessary to maintain the safety and security of the vessel. This includes denial of access to persons—except those identified as duly authorized by the cognizant government authority—or their effects, and refusal to load cargo, including containers or other closed cargo transport units.

(b) If, in the professional judgment of the Master, a conflict between any safety and security requirements applicable to the vessel arises during its operations, the Master may give precedence to measures intended to maintain the safety of the

vessel, and take such temporary security measures as seem best under all circumstances. In such cases:

(1) The Master must, as soon as practicable, inform the nearest COTP. If the vessel is on a foreign voyage, the Master must promptly inform the Coast Guard via the NRC at 1-800-424-8802, direct telephone at 202-267-2675, fax at 202-267-2165, TDD at 202-267-4477, or E-mail at lst-nrcinfo@comdt.uscg.mil and if subject to the jurisdiction of a foreign government, the relevant maritime authority of that foreign government;

(2) The temporary security measures must, to the highest possible degree, be commensurate with the prevailing Maritime Security (MARSEC) Level; and

(3) The owner or operator must ensure that such conflicts are resolved to the satisfaction of the cognizant COTP, or for vessels on international voyages, the Commandant (G-MP), and that the possibility of recurrence is minimized.

§ 104.210 Company Security Officer (CSO).

(a) *General.* (1) Each vessel owner or operator must designate in writing a CSO.

(2) A vessel owner or operator may designate a single CSO for all its vessels to which this part applies, or may designate more than one CSO, in which case the owner or operator must clearly identify the vessels for which each CSO is responsible.

(3) A CSO may perform other duties within the owner or operator's organization including the duties of a Vessel Security Officer, provided he or she is able to perform the duties and responsibilities required of a CSO.

(4) The CSO may delegate duties required by this part, but remains responsible for the performance of those duties.

(b) *Qualifications.* (1) The CSO must have general knowledge, through training or equivalent job experience, in the following:

(i) Security administration and organization of the company's vessel(s);

(ii) Vessel, facility, and port

operations relevant to that industry;

(iii) Vessel and facility security measures, including the meaning and the consequential requirements of the different Maritime Security (MARSEC) Levels;

(iv) Emergency preparedness and response and contingency planning;

(v) Security equipment and systems and their operational limitations;

(vi) Methods of conducting audits, inspection and control and monitoring techniques; and

(vii) Techniques for security training and education, including security measures and procedures.

(2) In addition to knowledge and training in paragraph (b)(1) of this section, the CSO must have general knowledge through training or equivalent job experience in the following, as appropriate:

(i) Relevant international conventions, codes, and recommendations;

(ii) Relevant government legislation and regulations;

(iii) Responsibilities and functions of other security organizations;

(iv) Methodology of Vessel Security Assessment;

(v) Methods of vessel security surveys and inspections;

(vi) Instruction techniques for security training and education, including security measures and procedures;

(vii) Handling sensitive security information and security related communications;

(viii) Knowledge of current security threats and patterns;

(ix) Recognition and detection of dangerous substances and devices;

(x) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

(xi) Techniques used to circumvent security measures;

(xii) Methods of physical screening and non-intrusive inspections;

(xiii) Security drills and exercises, including drills and exercises with facilities; and

(xiv) Assessment of security drills and exercises.

(c) *Responsibilities.* In addition to those responsibilities and duties specified elsewhere in this part, the CSO must, for each vessel for which he or she has been designated:

(1) Keep the vessel apprised of potential threats or other information relevant to its security;

(2) Ensure a Vessel Security Assessment (VSA) is carried out;

(3) Ensure a Vessel Security Plan (VSP) is developed, approved, and maintained;

(4) Ensure the VSP is modified when necessary;

(5) Ensure vessel security activities are audited;

(6) Arrange for Coast Guard inspections under 46 CFR part 2;

(7) Ensure the timely or prompt correction of problems identified by audits or inspections;

(8) Enhance security awareness and vigilance within the owner's or operator's organization;

(9) Ensure relevant personnel receive adequate security training;

(10) Ensure communication and cooperation between the vessel and the port and facilities with which the vessel interfaces;

(11) Ensure consistency between security requirements and safety requirements;

(12) Ensure that when sister-vessel or fleet security plans are used, the plan for each vessel reflects the vessel-specific information accurately;

(13) Ensure compliance with an Alternative Security Program or equivalents approved under this subchapter, if appropriate; and

(14) Ensure security measures give particular consideration to the convenience, comfort, and personal privacy of vessel personnel and their ability to maintain their effectiveness over long periods.

§ 104.215 Vessel Security Officer (VSO).

(a) *General.* (1) A VSO may perform other duties within the owner's or operator's organization, provided he or she is able to perform the duties and

responsibilities required of the VSO for each such vessel.

(2) For manned vessels, the VSO must be the Master or a member of the crew.

(3) For unmanned vessels, the VSO must be an employee of the company, and the same person may serve as the VSO for more than one unmanned vessel. If a person serves as the VSO for more than one unmanned vessel, the name of each unmanned vessel for which he or she is the VSO must be listed in the Vessel Security Plan (VSP).

(4) The VSO of any unmanned barge and the VSO of any towing vessel interfacing with the barge must coordinate and ensure the implementation of security measures applicable to both vessels during the period of their interface.

(5) The VSO may assign security duties to other vessel personnel; however, the VSO remains responsible for these duties.

(b) *Qualifications.* The VSO must have general knowledge, through training or equivalent job experience, in the following:

(1) Those items listed in §104.210 (b)(1) and (b)(2) of this part;

(2) Vessel layout;

(3) The VSP and related procedures, including scenario-based response training;

(4) Crowd management and control techniques;

(5) Operations of security equipment and systems; and

(6) Testing and calibration of security equipment and systems, and their maintenance while at sea.

(c) *Responsibilities.* In addition to those responsibilities and duties specified elsewhere in this part, the VSO must, for each vessel for which he or she has been designated:

(1) Regularly inspect the vessel to ensure that security measures are maintained;

(2) Ensure maintenance and supervision of the implementation of the VSP, and any amendments to the VSP;

(3) Ensure the coordination and handling of cargo and vessel stores and bunkers in compliance with this part;

(4) Propose modifications to the VSP to the Company Security Officer (CSO);

(5) Ensure that any problems identified during audits or inspections are reported to the CSO, and promptly implement any corrective actions;

(6) Ensure security awareness and vigilance on board the vessel;

(7) Ensure adequate security training for vessel personnel;

(8) Ensure the reporting and recording of all security incidents;

(9) Ensure the coordinated implementation of the VSP with the CSO and the relevant Facility Security Officer, when applicable;

(10) Ensure security equipment is properly operated, tested, calibrated and maintained; and

(11) Ensure consistency between security requirements and the proper treatment of vessel personnel affected by those requirements.

§ 104.220 Company or vessel personnel with security duties.

Company and vessel personnel responsible for security duties must have knowledge, through training or equivalent job experience, in the following, as appropriate:

(a) Knowledge of current security threats and patterns;

(b) Recognition and detection of dangerous substances and devices;

(c) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

(d) Techniques used to circumvent security measures;

(e) Crowd management and control techniques;

(f) Security related communications;

(g) Knowledge of emergency procedures and contingency plans;

(h) Operation of security equipment and systems;

(i) Testing and calibration of security equipment and systems, and their maintenance while at sea;

(j) Inspection, control, and monitoring techniques;

(k) Relevant provisions of the Vessel Security Plan (VSP);

(l) Methods of physical screening of persons, personal effects, baggage, cargo, and vessel stores; and

(m) The meaning and the consequential requirements of the different Maritime Security (MARSEC) Levels.

§ 104.225 Security training for all other vessel personnel.

All other vessel personnel, including contractors, whether part-time, full-time, temporary, or permanent, must have knowledge of, through training or equivalent job experience in the following, as appropriate:

(a) Relevant provisions of the Vessel Security Plan (VSP);

(b) The meaning and the consequential requirements of the different Maritime Security (MARSEC) Levels, including emergency procedures and contingency plans;

(c) Recognition and detection of dangerous substances and devices;

(d) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security; and

(e) Techniques used to circumvent security measures.

§ 104.230 Drill and exercise requirements.

(a) *General.* (1) Drills and exercises must test the proficiency of vessel personnel in assigned security duties at all Maritime Security (MARSEC) Levels and the effective implementation of the Vessel Security Plan (VSP). They must enable the Vessel Security Officer (VSO) to identify any related security deficiencies that need to be addressed.

(2) A drill or exercise required by this section may be satisfied with the implementation of security measures required by the Vessel Security Plan as the result of an increase in the MARSEC Level, provided the vessel reports attainment to the cognizant COTP.

(b) *Drills.* (1) The VSO must ensure that at least one security drill is conducted at least every 3 months, except when a vessel is out of service

due to repairs or seasonal suspension of operation provided that in such cases a drill must be conducted within one week of the vessel's reactivation. Security drills may be held in conjunction with non-security drills where appropriate.

(2) Drills must test individual elements of the VSP, including response to security threats and incidents. Drills should take into account the types of operations of the vessel, vessel personnel changes, and other relevant circumstances. Examples of drills include unauthorized entry to a restricted area, response to alarms, and notification of law enforcement authorities.

(3) If the vessel is moored at a facility on the date the facility has planned to conduct any drills, the vessel may, but is not required to, participate in the facility's scheduled drill.

(4) Drills must be conducted within one week from whenever the percentage of vessel personnel with no prior participation in a vessel security drill on that vessel exceeds 25 percent.

(5) Notwithstanding paragraph (b)(4) of this section, vessels not subject to SOLAS may conduct drills within 1 week from whenever the percentage of vessel personnel with no prior participation in a vessel security drill on a vessel of similar design and owned or operated by the same company exceeds 25 percent.

(c) *Exercises.* (1) Exercises must be conducted at least once each calendar year, with no more than 18 months between exercises.

(2) Exercises may be:

(i) Full scale or live;

(ii) Tabletop simulation or seminar;

(iii) Combined with other appropriate exercises; or

(iv) A combination of the elements in paragraphs (c)(2)(i) through (iii) of this section.

(3) Exercises may be vessel-specific or part of a cooperative exercise program to exercise applicable facility and vessel security plans or comprehensive port exercises.

(4) Each exercise must test communication and notification procedures, and elements of

coordination, resource availability, and response.

(5) Exercises are a full test of the security program and must include the substantial and active participation of relevant company and vessel security personnel, and may include facility security personnel and government authorities depending on the scope and the nature of the exercises.

§ 104.235 Vessel recordkeeping requirements.

(a) Unless otherwise specified in this section, the Vessel Security Officer must keep records of the activities as set out in paragraph (b) of this section for at least 2 years and make them available to the Coast Guard upon request.

(b) Records required by this section may be kept in electronic format. If kept in an electronic format, they must be protected against unauthorized deletion, destruction, or amendment. The following records must be kept:

(1) *Training.* For training under § 104.225, the date of each session, duration of session, a description of the training, and a list of attendees;

(2) *Drills and exercises.* For each drill or exercise, the date held, description of drill or exercise, list of participants; and any best practices or lessons learned which may improve the Vessel Security Plan (VSP);

(3) *Incidents and breaches of security.* Date and time of occurrence, location within the port, location within the vessel, description of incident or breaches, to whom it was reported, and description of the response;

(4) *Changes in Maritime Security (MARSEC) Levels.* Date and time of notification received, and time of compliance with additional requirements;

(5) *Maintenance, calibration, and testing of security equipment.* For each occurrence of maintenance, calibration, and testing, the date and time, and the specific security equipment involved;

(6) *Security threats.* Date and time of occurrence, how the threat was communicated, who received or

identified the threat, description of threat, to whom it was reported, and description of the response;

(7) *Declaration of Security (DoS).* Manned vessels must keep on board a copy of the last 10 DoSs and a copy of each continuing DoS for at least 90 days after the end of its effective period; and

(8) *Annual audit of the VSP.* For each annual audit, a letter certified by the Company Security Officer or the VSO stating the date the audit was completed.

(c) Any records required by this part must be protected from unauthorized access or disclosure.

§ 104.240 Maritime Security (MARSEC) Level coordination and implementation.

(a) The vessel owner or operator must ensure that, prior to entering a port or visiting an Outer Continental Shelf (OCS) facility, all measures are taken that are specified in the Vessel Security Plan (VSP) for compliance with the MARSEC Level in effect for the port or the OCS facility.

(b) When notified of an increase in the MARSEC Level, the vessel owner or operator must ensure:

(1) If a higher MARSEC Level is set for the port in which the vessel is located or is about to enter, the vessel complies, without undue delay, with all measures specified in the VSP for compliance with that higher MARSEC Level;

(2) The COTP is notified as required by §101.300(c) when compliance with the higher MARSEC Level has been implemented;

(3) For vessels in port, that compliance with the higher MARSEC Level has taken place within 12 hours of the notification; and

(4) If a higher MARSEC Level is set for the OCS facility with which the vessel is interfacing or is about to visit, the vessel complies, without undue delay, with all measures specified in the VSP for compliance with that higher MARSEC Level.

(c) For MARSEC Levels 2 and 3, the Vessel Security Officer must brief all vessel personnel of identified threats,

emphasize reporting procedures, and stress the need for increased vigilance.

(d) An owner or operator whose vessel is not in compliance with the requirements of this section must inform the COTP and obtain approval prior to entering any port, prior to interfacing with another vessel or with a facility or to continuing operations.

(e) For MARSEC Level 3, in addition to the requirements in this part, a vessel owner or operator may be required to implement additional measures, pursuant to 33 CFR part 6, 160 or 165, as appropriate, which may include but are not limited to:

(1) Arrangements to ensure that the vessel can be towed or moved if deemed necessary by the Coast Guard;

(2) Use of waterborne security patrol;

(3) Use of armed security personnel to control access to the vessel and to deter, to the maximum extent practical, a TSI; or

(4) Screening the vessel for the presence of dangerous substances and devices underwater or other threats.

§ 104.245 Communications.

(a) The Vessel Security Officer must have a means to effectively notify vessel personnel of changes in security conditions on board the vessel.

(b) Communications systems and procedures must allow effective and continuous communication between the vessel security personnel, facilities interfacing with the vessel, vessels interfacing with the vessel, and national or local authorities with security responsibilities.

(c) Communication systems and procedures must enable vessel personnel to notify, in a timely manner, shore side authorities or other vessels of a security threat or incident on board.

§ 104.250 Procedures for interfacing with facilities and other vessels.

(a) The vessel owner or operator must ensure that there are measures for interfacing with facilities and other vessels at all MARSEC Levels.

(b) For each U.S. flag vessel that calls on foreign ports or facilities, the

vessel owner or operator must ensure procedures for interfacing with those ports and facilities are established.

§ 104.255 Declaration of Security (DoS).

(a) Each vessel owner or operator must ensure procedures are established for requesting a DoS and for handling DoS requests from a facility or other vessel.

(b) At MARSEC Level 1, the Master or Vessel Security Officer (VSO), or their designated representative, of any cruise ship or manned vessel carrying Certain Dangerous Cargoes, in bulk, must complete and sign a DoS with the VSO or Facility Security Officer (FSO), or their designated representative, of any vessel or facility with which it interfaces.

(1) For a vessel-to-facility interface, prior to arrival of a vessel to a facility, the FSO and Master, VSO, or their designated representatives must coordinate security needs and procedures, and agree upon the contents of the DoS for the period of time the vessel is at the facility. Upon a vessel's arrival to a facility and prior to any passenger embarkation or disembarkation or cargo transfer operation, the FSO or Master, VSO, or designated representatives must sign the written DoS.

(2) For a vessel engaging in a vessel-to-vessel activity, prior to the activity, the respective Masters, VSOs, or their designated representatives must coordinate security needs and procedures, and agree upon the contents of the DoS for the period of the vessel-to-vessel activity. Upon the vessel-to-vessel activity and prior to any passenger embarkation or disembarkation or cargo transfer operation, the respective Masters, VSOs, or designated representatives must sign the written DoS.

(c) At MARSEC Levels 2 and 3, the Master, VSO, or designated representative of any manned vessel required to comply with this part must coordinate security needs and procedures, and agree upon the contents of the DoS for the period of the vessel-

to-vessel activity. Upon the vessel-to-vessel activity and prior to any passenger embarkation or disembarkation or cargo transfer operation, the respective Masters, VSOs, or designated representatives must sign the written DoS.

(d) At MARSEC Levels 2 and 3, the Master, VSO, or designated representative of any manned vessel required to comply with this part must coordinate security needs and procedures, and agree upon the contents of the DoS for the period the vessel is at the facility. Upon the vessel's arrival to a facility and prior to any passenger embarkation or disembarkation or cargo transfer operation, the respective FSO and Master, VSO, or designated representatives must sign the written DoS.

(e) At MARSEC Levels 1 and 2, VSOs of vessels that frequently interface with the same facility may implement a continuing DoS for multiple visits, provided that:

(1) The DoS is valid for the specific MARSEC Level;

(2) The effective period at MARSEC Level 1 does not exceed 90 days; and

(3) The effective period at MARSEC Level 2 does not exceed 30 days.

(f) When the MARSEC Level increases beyond the level contained in the DoS, the continuing DoS becomes void and a new DoS must be signed and implemented in accordance with this section.

(g) The COTP may require at any time, at any MARSEC Level, any manned vessel subject to this part to implement a DoS with the VSO or FSO prior to any vessel-to-vessel activity or vessel-to-facility interface when he or she deems it necessary.

§ 104.260 Security systems and equipment maintenance.

(a) Security systems and equipment must be in good working order and inspected, tested, calibrated and maintained according to the manufacturer's recommendation.

(b) The results of testing completed under paragraph (a) of this

section shall be recorded in accordance with §104.235. Any deficiencies shall be promptly corrected.

(c) The Vessel Security Plan (VSP) must include procedures for identifying and responding to security system and equipment failures or malfunctions.

§ 104.265 Security measures for access control.

(a) *General.* The vessel owner or operator must ensure the implementation of security measures to:

(1) Deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, facilities, or ports;

(2) Secure dangerous substances and devices that are authorized by the owner or operator to be on board; and

(3) Control access to the vessel.

(b) The vessel owner or operator must ensure that the following are specified:

(1) The locations providing means of access to the vessel where access restrictions or prohibitions are applied for each Maritime Security (MARSEC) Level. "Means of access" include, but are not limited, to all:

(i) Access ladders;

(ii) Access gangways;

(iii) Access ramps;

(iv) Access doors, side scuttles, windows, and ports;

(v) Mooring lines and anchor chains; and

(vi) Cranes and hoisting gear;

(2) The identification of the types of restriction or prohibition to be applied and the means of enforcing them; and

(3) The means of identification required to allow individuals to access the vessel and remain on the vessel without challenge.

(c) The vessel owner or operator must ensure that an identification system is established for checking the identification of vessel personnel or other persons seeking access to the vessel that:

(1) Allows identification of authorized and unauthorized persons at any MARSEC Level;

(2) Is coordinated, when practicable, with identification systems at facilities used by the vessel;

(3) Is updated regularly;

(4) Uses disciplinary measures to discourage abuse;

(5) Allows temporary or continuing access for vessel personnel and visitors, including seafarers' chaplains and union representatives, through the use of a badge or other system to verify their identity; and

(6) Allow certain long-term, frequent vendor representatives to be treated more as employees than as visitors.

(d) The vessel owner or operator must establish in the approved Vessel Security Plan (VSP) the frequency of application of any security measures for access control, particularly if these security measures are applied on a random or occasional basis.

(e) *MARSEC Level 1*. The vessel owner or operator must ensure security measures in this paragraph are implemented to:

(1) Screen persons, baggage (including carry-on items), personal effects, and vehicles for dangerous substances and devices at the rate specified in the approved Vessels Security Plan (VSP), except for government-owned vehicles on official business when government personnel present identification credentials for entry;

(2) Conspicuously post signs that describe security measures currently in effect and clearly state that:

(i) Boarding the vessel is deemed valid consent to screening or inspection; and

(ii) Failure to consent or submit to screening or inspection will result in denial or revocation of authorization to board;

(3) Check the identification of any person seeking to board the vessel, including vessel passengers and crew, facility employees, vendors, personnel duly authorized by the cognizant government authorities, and visitors. This check includes confirming the reason for boarding by examining at least one of the following:

(i) Joining instructions;

(ii) Passenger tickets;

(iii) Boarding passes;

(iv) Work orders, pilot orders, or surveyor orders;

(v) Government identification;

or

(vi) Visitor badges issued in accordance with an identification system required in paragraph (c) of this section;

(4) Deny or revoke a person's authorization to be on board if the person is unable or unwilling, upon the request of vessel personnel, to establish his or her identity or to account for his or her presence on board. Any such incident must be reported in compliance with this part;

(5) Deter unauthorized access to the vessel;

(6) Identify access points that must be secured or attended to deter unauthorized access;

(7) Lock or otherwise prevent access to unattended spaces that adjoin areas to which passengers and visitors have access;

(8) Provide a designated secure area on board or in liaison with a facility, for conducting inspections and screening of people, baggage (including carry-on items), personal effects, vehicles and the vehicle's contents;

(9) Ensure vessel personnel are not subjected to screening, of the person or of personal effects, by other vessel personnel, unless security clearly requires it. Any such screening must be conducted in a way that takes into full account individual human rights and preserves the individual's basic human dignity;

(10) Ensure the screening of all unaccompanied baggage;

(11) Ensure checked persons and their personal effects are segregated from unchecked persons and their personal effects;

(12) Ensure embarking passengers are segregated from disembarking passengers;

(13) Ensure, in liaison with the facility, a defined percentage of vehicles to be loaded aboard passenger vessels are screened prior to loading at the rate specified in the approved VSP;

(14) Ensure, in liaison with the facility, all unaccompanied vehicles to be loaded on passenger vessels are

screened prior to loading; and

(15) Respond to the presence of unauthorized persons on board, including repelling unauthorized boarders.

(f) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the vessel owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved VSP. These additional security measures may include:

(1) Increasing the frequency and detail of screening of people, personal effects, and vehicles being embarked or loaded onto the vessel as specified for MARSEC Level 2 in the approved VSP, except for government-owned vehicles on official business when government personnel present identification credentials for entry;

(2) X-ray screening of all unaccompanied baggage;

(3) Assigning additional personnel to patrol deck areas during periods of reduced vessel operations to deter unauthorized access;

(4) Limiting the number of access points to the vessel by closing and securing some access points;

(5) Denying access to visitors who do not have a verified destination;

(6) Deterring waterside access to the vessel, which may include, in liaison with the facility, providing boat patrols; and

(7) Establishing a restricted area on the shoreside of the vessel, in close cooperation with the facility.

(g) *MARSEC Level 3.* In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, the vessel owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved VSP. The additional security measures may include:

(1) Screening all persons, baggage, and personal effects for dangerous substances and devices;

(2) Performing one or more of the following on unaccompanied baggage:

(i) Screen unaccompanied

baggage more extensively, for example, x-raying from two or more angles;

(ii) Prepare to restrict or suspend handling unaccompanied baggage; or

(iii) Refuse to accept unaccompanied baggage on board;

(3) Being prepared to cooperate with responders and facilities;

(4) Limiting access to the vessel to a single, controlled access point;

(5) Granting access to only those responding to the security incident or threat thereof;

(6) Suspending embarkation and/or disembarkation of personnel;

(7) Suspending cargo operations;

(8) Evacuating the vessel;

(9) Moving the vessel; and

(10) Preparing for a full or partial search of the vessel.

§ 104.270 Security measures for restricted areas.

(a) *General.* The vessel owner or operator must ensure the designation of restricted areas in order to:

(1) Prevent or deter unauthorized access;

(2) Protect persons authorized to be on board;

(3) Protect the vessel;

(4) Protect sensitive security areas within the vessel;

(5) Protect security and surveillance equipment and systems; and

(6) Protect cargo and vessel stores from tampering.

(b) *Designation of Restricted Areas.* The vessel owner or operator must ensure restricted areas are designated on board the vessel, as specified in the approved plan. Restricted areas must include, as appropriate:

(1) Navigation bridge, machinery spaces and other control stations;

(2) Spaces containing security and surveillance equipment and systems and their controls and lighting system controls;

(3) Ventilation and air-conditioning systems and other similar spaces;

(4) Spaces with access to potable

water tanks, pumps, or manifolds;

(5) Spaces containing dangerous goods or hazardous substances;

(6) Spaces containing cargo pumps and their controls;

(7) Cargo spaces and spaces containing vessel stores;

(8) Crew accommodations; and

(9) Any other spaces or areas vital to the security of the vessel.

(c) The vessel owner or operator must ensure that security measures and policies are established to:

(1) Identify which vessel personnel are authorized to have access;

(2) Determine which persons other than vessel personnel are authorized to have access;

(3) Determine the conditions under which that access may take place;

(4) Define the extent of any restricted area;

(5) Define the times when access restrictions apply; and

(6) Clearly mark all restricted areas and indicate that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security.

(d) *Maritime Security (MARSEC) Level 1.* The vessel owner or operator must ensure the implementation of security measures to prevent unauthorized access or activities within the area. These security measures may include:

(1) Locking or securing access points;

(2) Monitoring and using surveillance equipment;

(3) Using guards or patrols; and

(4) Using automatic intrusion detection devices, which if used must activate an audible and/or visual alarm at a location that is continuously attended or monitored, to alert vessel personnel to unauthorized access.

(e) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the vessel owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved VSP. These additional security measures may include:

(1) Increasing the frequency and

intensity of monitoring and access controls on existing restricted access areas;

(2) Restricting access to areas adjacent to access points;

(3) Providing continuous monitoring of each area, using surveillance equipment; and

(4) Dedicating additional personnel to guard or patrol each area.

(f) *MARSEC Level 3.* In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the vessel owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved VSP. These additional security measures may include:

(1) Restricting access to additional areas; and

(2) Searching restricted areas as part of a security sweep of the vessel.

§ 104.275 Security measures for handling cargo.

(a) General. The vessel owner or operator must ensure that security measures relating to cargo handling, some of which may have to be applied in liaison with the facility or another vessel, are specified in order to:

(1) Deter tampering;

(2) Prevent cargo that is not meant for carriage from being accepted and stored on board the vessel;

(3) Identify cargo that is approved for loading onto the vessel;

(4) Include inventory control procedures at access points to the vessel; and

(5) When there are regular or repeated cargo operations with the same shipper, coordinate security measures with the shipper or other responsible party in accordance with an established agreement and procedures.

(b) *Maritime Security (MARSEC) Level 1.* At MARSEC Level 1, the vessel owner or operator must ensure the implementation of measures to:

(1) Unless unsafe to do so, routinely check cargo and cargo spaces prior to and during cargo handling for evidence of tampering;

(2) Check that cargo to be loaded matches the cargo documentation, or that cargo markings or container numbers match the information provided with shipping documents;

(3) Ensure, in liaison with the facility, that vehicles to be loaded on board car carriers, RO-RO, and passenger ships are subjected to screening prior to loading, in accordance with the frequency required in the VSP; and

(4) Check, in liaison with the facility, seals or other methods used to prevent tampering.

(c) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the vessel owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved Vessel Security Plan (VSP). These additional security measures may include:

(1) Increasing the frequency and detail of checking cargo and cargo spaces for evidence of tampering;

(2) Intensifying checks to ensure that only the intended cargo, container, or other cargo transport units are loaded;

(3) Intensifying screening of vehicles to be loaded on car-carriers, RO-RO, and passenger vessels;

(4) In liaison with the facility, increasing frequency and detail in checking seals or other methods used to prevent tampering;

(5) Increasing the frequency and intensity of visual and physical inspections; or

(6) Coordinating enhanced security measures with the shipper or other responsible party in accordance with an established agreement and procedures.

(d) *MARSEC Level 3.* In addition to the security measures for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the vessel owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved VSP. These additional security measures may include:

(1) Suspending loading or

unloading of cargo;

(2) Being prepared to cooperate with responders, facilities, and other vessels; or

(3) Verifying the inventory and location of any hazardous materials carried on board.

§ 104.280 Security measures for delivery of vessel stores and bunkers.

(a) *General.* The vessel owner or operator must ensure that security measures relating to the delivery of vessel stores and bunkers are implemented to:

(1) Check vessel stores for package integrity;

(2) Prevent vessel stores from being accepted without inspection;

(3) Deter tampering; and

(4) Prevent vessel stores and bunkers from being accepted unless ordered. For vessels that routinely use a facility, a vessel owner or operator may establish and implement standing arrangements between the vessel, its suppliers, and a facility regarding notification and the timing of deliveries and their documentation.

(b) *Maritime Security (MARSEC) Level 1.* At MARSEC Level 1, the vessel owner or operator must ensure the implementation of measures to:

(1) Check vessel stores before being accepted;

(2) Check that vessel stores and bunkers match the order prior to being brought on board or being bunkered; and

(3) Ensure that vessel stores are controlled or immediately and securely stowed following delivery.

(c) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the vessel owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved Vessel Security Plan (VSP). These additional security measures may include:

(1) Intensifying inspection of the vessel stores during delivery; or

(2) Checking vessel stores prior

to receiving them on board.

(d) *MARSEC Level 3*. In addition to the security measures for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the vessel owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved VSP. These additional security measures may include:

- (1) Checking all vessel stores more extensively;
- (2) Restricting or suspending delivery of vessel stores and bunkers; or
- (3) Refusing to accept vessel stores on board.

§ 104.285 Security measures for monitoring.

(a) *General*. (1) The vessel owner or operator must ensure the implementation of security measures and have the capability to continuously monitor, through a combination of lighting, watchkeepers, security guards, deck watches, waterborne patrols, automatic intrusion-detection devices, or surveillance equipment, as specified in their approved Vessel Security Plan (VSP), the—

- (i) Vessel;
- (ii) Restricted areas on board the vessel; and
- (iii) Area surrounding the vessel.

(2) The following must be considered when establishing the appropriate level and location of lighting:

- (i) Vessel personnel should be able to detect activities on and around the vessel, on both the shore side and the waterside;
- (ii) Coverage should facilitate personnel identification at access points;
- (iii) Coverage may be provided through coordination with the port or facility; and
- (iv) Lighting effects, such as glare, and its impact on safety, navigation, and other security activities.

(b) *Maritime Security (MARSEC) Level 1*. At MARSEC Level 1, the vessel owner or operator must ensure the implementation of security

measures, which may be done in coordination with a facility, to:

(1) Monitor the vessel, particularly vessel access points and restricted areas;

(2) Be able to conduct emergency searches of the vessel;

(3) Ensure that equipment or system failures or malfunctions are identified and corrected;

(4) Ensure that any automatic intrusion detection device sets off an audible or visual alarm, or both, at a location that is continuously attended or monitored;

(5) Light deck and vessel access points during the period between sunset and sunrise and periods of limited visibility sufficiently to allow visual identification of persons seeking access to the vessel; and

(6) Use maximum available lighting while underway, during the period between sunset and sunrise, consistent with safety and international regulations.

(c) *MARSEC Level 2*. In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the vessel owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved VSP. These additional security measures may include:

(1) Increasing the frequency and detail of security patrols;

(2) Increasing the coverage and intensity of lighting, alone or in coordination with the facility;

(3) Using or increasing the use of security and surveillance equipment;

(4) Assigning additional personnel as security lookouts;

(5) Coordinating with boat patrols, when provided; and

(6) Coordinating with shoreside foot or vehicle patrols, when provided.

(d) *MARSEC Level 3*. In addition to the security measures for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the vessel owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved VSP. These additional security measures may

include:

- (1) Cooperating with responders and facilities;
- (2) Switching on all lights;
- (3) Illuminating the vicinity of the vessel;
- (4) Switching on all surveillance equipment capable of recording activities on, or in the vicinity of, the vessel;
- (5) Maximizing the length of time such surveillance equipment can continue to record;
- (6) Preparing for underwater inspection of the hull; and
- (7) Initiating measures, including the slow revolution of the vessel's propellers, if practicable, to deter underwater access to the hull of the vessel.

§ 104.290 Security incident procedures.

For each Maritime Security (MARSEC) Level, the vessel owner or operator must ensure the Vessel Security Officer (VSO) and vessel security personnel are able to:

(a) Respond to security threats or breaches of security and maintain critical vessel and vessel-to-facility interface operations, to include:

- (1) Prohibiting entry into affected area;
- (2) Denying access to the vessel, except to those responding to the emergency;
- (3) Implementing MARSEC Level 3 security measures throughout the vessel;
- (4) Stopping cargo-handling operations; and
- (5) Notifying shoreside authorities or other vessels of the emergency;

(b) Evacuating the vessel in case of security threats or breaches of security;

(c) Reporting security incidents as required in §101.305;

(d) Briefing all vessel personnel on possible threats and the need for vigilance, soliciting their assistance in reporting suspicious persons, objects, or activities; and

(e) Securing non-critical operations in order to focus response

on critical operations.

§ 104.292 Additional requirements—passenger vessels and ferries.

(a) At all Maritime Security (MARSEC) Levels, the vessel owner or operator must ensure security sweeps are performed, prior to getting underway, after any period the vessel was unattended.

(b) As an alternative to the identification checks and passenger screening requirements in §104.265 (e)(1), (e)(3), and (e)(8), the owner or operator of a passenger vessel or ferry may ensure security measures are implemented that include:

(1) Searching selected areas prior to embarking passengers and prior to sailing; and

(2) Implementing one or more of the following:

(i) Performing routine security patrols;

(ii) Providing additional closed-circuit television to monitor passenger areas; or

(iii) Securing all non-passenger areas.

(c) Passenger vessels certificated to carry more than 2000 passengers, working in coordination with the terminal, may be subject to additional vehicle screening requirements in accordance with a MARSEC Directive or other orders issued by the Coast Guard.

(d) Owners and operators of passenger vessels and ferries covered by this part that use public access facilities, as that term is defined in § 101.105 of this subchapter, must address security measures for the interface of the vessel and the public access facility, in accordance with the appropriate Area Maritime Security Plan.

(e) At MARSEC Level 2, a vessel owner or operator must ensure, in addition to MARSEC Level 1 measures, the implementation of the following:

(1) Search selected areas prior to embarking passengers and prior to sailing;

(2) Passenger vessels certificated

to carry less than 2000 passengers, working in coordination with the terminal, may be subject to additional vehicle screening requirements in accordance with a MARSEC Directive or other orders issued by the Coast Guard; and

(3) As an alternative to the identification and screening requirements in §104.265(e)(3) and (f)(1), intensify patrols, security sweeps and monitoring identified in paragraph (b) of this section.

(f) At MARSEC Level 3, a vessel owner or operator may, in addition to MARSEC Levels 1 and 2 measures, as an alternative to the identification checks and passenger screening requirements in §104.265(e)(3) and §104.265(g)(1), ensure that random armed security patrols are conducted, which need not consist of vessel personnel.

§ 104.295 Additional requirements—cruise ships.

(a) At all MARSEC Levels, the owner or operator of a cruise ship must ensure the following:

(1) Screen all persons, baggage, and personal effects for dangerous substances and devices;

(2) Check the identification of all persons seeking to board the vessel; this check includes confirming the reason for boarding by examining joining instructions, passenger tickets, boarding passes, government identification or visitor badges, or work orders;

(3) Perform security patrols; and

(4) Search selected areas prior to embarking passengers and prior to sailing.

(b) At MARSEC Level 3, the owner or operator of a cruise ship must ensure that security briefs to passengers about the specific threat are provided.

§ 104.297 Additional requirements—vessels on international voyages.

(a) An owner or operator of a U.S. flag vessel, which is subject to the International Convention for Safety of Life at Sea, 1974, (SOLAS), must be in compliance with the applicable requirements of SOLAS Chapter XI-

1, SOLAS Chapter XI-2 and the ISPS Code, part A (Incorporated by reference, see §101.115 of this subchapter).

(b) Owners or operators of U.S. flag vessels that are required to comply with SOLAS, must ensure an International Ship Security Certificate (ISSC) as provided in 46 CFR §2.01-25 is obtained for the vessel. This certificate must be issued by the Coast Guard.

(c) Owners or operators of vessels that require an ISSC in paragraph (b) of this section must request an inspection in writing, at least 30 days prior to the desired inspection date to the Officer in Charge, Marine Inspection for the Marine Inspection Office or Marine Safety Office of the port where the vessel will be inspected to verify compliance with this part and applicable SOLAS requirements. The inspection must be completed and the initial ISSC must be issued on or before July 1, 2004.

Subpart C—Vessel Security Assessment (VSA)

§ 104.300 General.

(a) The Vessel Security Assessment (VSA) is a written document that is based on the collection of background information and the completion and analysis of an on-scene survey.

(b) A single VSA may be performed and applied to more than one vessel to the extent that they share physical characteristics and operations.

(c) Third parties may be used in any aspect of the VSA if they have the appropriate skills and if the Company Security Officer (CSO) reviews and accepts their work.

(d) Those involved in a VSA should be able to draw upon expert assistance in the following areas:

(1) Knowledge of current security threats and patterns;

(2) Recognition and detection of dangerous substances and devices;

(3) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

(4) Techniques used to

circumvent security measures;

(5) Methods used to cause a security incident;

(6) Effects of dangerous substances and devices on vessel structures and equipment;

(7) Vessel security requirements;

(8) Vessel-to-vessel activity and vessel-to-facility interface business practices;

(9) Contingency planning, emergency preparedness and response;

(10) Physical security requirements;

(11) Radio and telecommunications systems, including computer systems and networks;

(12) Marine engineering; and

(13) Vessel and port operations.

§ 104.305 Vessel Security Assessment (VSA) requirements.

(a) *Background.* The vessel owner or operator must ensure that the following background information is provided to the person or persons who will conduct the on-scene survey and assessment:

(1) General layout of the vessel, including the location of:

(i) Each actual or potential point of access to the vessel and its function;

(ii) Spaces that should have restricted access;

(iii) Essential maintenance equipment;

(iv) Cargo spaces and storage;

(v) Storage of unaccompanied baggage; and

(vi) Vessel stores;

(2) Threat assessments, including the purpose and methodology of the assessment, for the area or areas in which the vessel operates or at which passengers embark or disembark;

(3) The previous VSA, if any;

(4) Emergency and stand-by equipment available to maintain essential services;

(5) Number of vessel personnel and any existing security duties to which they are assigned;

(6) Existing personnel training requirement practices of the vessel;

(7) Existing security and safety equipment for the protection of personnel, visitors, passengers, and

vessels personnel;

(8) Escape and evacuation routes and assembly stations that have to be maintained to ensure the orderly and safe emergency evacuation of the vessel;

(9) Existing agreements with private security companies providing waterside or vessel security services; and

(10) Existing security measures and procedures, including:

(i) Inspection and control procedures;

(ii) Identification systems;

(iii) Surveillance and monitoring equipment;

(iv) Personnel identification documents;

(v) Communication systems;

(vi) Alarms;

(vii) Lighting;

(viii) Access control systems; and

(ix) Other security systems.

(b) *On-scene survey.* The vessel owner or operator must ensure that an on-scene survey of each vessel is conducted. The on-scene survey is to verify or collect information required in paragraph (a) of this section. It consists of an actual survey that examines and evaluates existing vessel protective measures, procedures, and operations for:

(1) Ensuring performance of all security duties;

(2) Controlling access to the vessel, through the use of identification systems or otherwise;

(3) Controlling the embarkation of vessel personnel and other persons and their effects, including personal effects and baggage whether accompanied or unaccompanied;

(4) Supervising the handling of cargo and the delivery of vessel stores;

(5) Monitoring restricted areas to ensure that only authorized persons have access;

(6) Monitoring deck areas and areas surrounding the vessel; and

(7) The ready availability of security communications, information, and equipment.

(c) *Analysis and recommendations.* In conducting the VSA, the Company Security Officer (CSO) must analyze the vessel

background information and the on-scene survey, and while considering the requirements of this part, provide recommendations for the security measures the vessel should include in the Vessel Security Plan (VSP). This includes but is not limited to the following:

- (1) Restricted areas;
- (2) Response procedures for fire or other emergency conditions;
- (3) Security supervision of vessel personnel, passengers, visitors, vendors, repair technicians, dock workers, etc.;
- (4) Frequency and effectiveness of security patrols;
- (5) Access control systems, including identification systems;
- (6) Security communication systems and procedures;
- (7) Security doors, barriers, and lighting;
- (8) Any security and surveillance equipment and systems;
- (9) Possible security threats, including but not limited to:
 - (i) Damage to or destruction of the vessel or an interfacing facility or vessel by dangerous substances and devices, arson, sabotage, or vandalism;
 - (ii) Hijacking or seizure of the vessel or of persons on board;
 - (iii) Tampering with cargo, essential vessel equipment or systems, or vessel stores;
 - (iv) Unauthorized access or use, including presence of stowaways;
 - (v) Smuggling dangerous substances and devices;
 - (vi) Use of the vessel to carry those intending to cause a security incident and/or their equipment;
 - (vii) Use of the vessel itself as a weapon or as a means to cause damage or destruction;
 - (viii) Attacks from seaward while at berth or at anchor; and
 - (ix) Attacks while at sea; and
- (10) Evaluating the potential of each identified point of access, including open weather decks, for use by individuals who might seek to breach security, whether or not those individuals legitimately have access to the vessel.

(d) *VSA report.* (1) The vessel owner or operator must ensure that a

written VSA report is prepared and included as part of the VSP. The VSA report must contain:

- (i) A summary of how the on-scene survey was conducted;
- (ii) Existing security measures, procedures, and operations;
- (iii) A description of each vulnerability found during the assessment;
- (iv) A description of security countermeasures that could be used to address each vulnerability;
- (v) A list of the key vessel operations that are important to protect;
- (vi) The likelihood of possible threats to key vessel operations; and
- (vii) A list of identified weaknesses, including human factors, in the infrastructure, policies, and procedures of the vessel.

(2) The VSA report must address the following elements on board or within the vessel:

- (i) Physical security;
 - (ii) Structural integrity;
 - (iii) Personnel protection systems;
 - (iv) Procedural policies;
 - (v) Radio and telecommunication systems, including computer systems and networks; and
 - (vi) Other areas that may, if damaged or used illicitly, pose a risk to people, property, or operations on board the vessel or within a facility.
- (3) The VSA report must list the persons, activities, services, and operations that are important to protect, in each of the following categories:
- (i) Vessel personnel;
 - (ii) Passengers, visitors, vendors, repair technicians, facility personnel, etc.;
 - (iii) Capacity to maintain safe navigation and emergency response;
 - (iv) Cargo, particularly dangerous goods and hazardous substances;
 - (v) Vessel stores;
 - (vi) Any vessel security communication and surveillance systems; and
 - (vii) Any other vessel security systems, if any.

(4) The VSA report must account for any vulnerabilities in the following areas:

(i) Conflicts between safety and security measures;

(ii) Conflicts between vessel duties and security assignments;

(iii) The impact of watch-keeping duties and risk of fatigue on vessel personnel alertness and performance;

(iv) Security training deficiencies; and

(v) Security equipment and systems, including communication systems.

(5) The VSA report must discuss and evaluate key vessel measures and operations, including:

(i) Ensuring performance of all security duties;

(ii) Controlling access to the vessel, through the use of identification systems or otherwise;

(iii) Controlling the embarkation of vessel personnel and other persons and their effects (including personal effects and baggage whether accompanied or unaccompanied);

(iv) Supervising the handling of cargo and the delivery of vessel stores;

(v) Monitoring restricted areas to ensure that only authorized persons have access;

(vi) Monitoring deck areas and areas surrounding the vessel; and

(vii) The ready availability of security communications, information, and equipment.

(e) The VSA must be documented and the VSA report retained by the vessel owner or operator with the VSP. The VSA, the VSA report, and VSP must be protected from unauthorized access or disclosure.

§ 104.310 Submission requirements.

(a) A completed Vessel Security Assessment (VSA) report must be submitted with the Vessel Security Plan (VSP) required in § 104.410 of this part.

(b) A vessel owner or operator may generate and submit a report that contains the VSA for more than one vessel subject to this part, to the extent that they share similarities in physical characteristics and operations.

(c) The VSA must be reviewed and revalidated, and the VSA report must be updated, each time the VSP is

submitted for reapproval or revisions.

Subpart D—Vessel Security Plan (VSP)

§ 104.400 General.

(a) The Company Security Officer (CSO) must ensure a Vessel Security Plan (VSP) is developed and implemented for each vessel. The VSP:

(1) Must identify the CSO and VSO by name or position and provide 24-hour contact information;

(2) Must be written in English, although a translation of the VSP in the working language of vessel personnel may also be developed;

(3) Must address each vulnerability identified in the Vessel Security Assessment (VSA);

(4) Must describe security measures for each MARSEC Level;

(5) Must state the Master's authority as described in § 104.205; and

(6) May cover more than one vessel to the extent that they share similarities in physical characteristics and operations, if authorized and approved by the Commanding Officer, Marine Safety Center.

(b) The VSP must be submitted to the Commanding Officer, Marine Safety Center (MSC) 400 Seventh Street, SW, Room 6302, Nassif Building, Washington, DC 20590-0001, in a written or electronic format. Information for submitting the VSP electronically can be found at <http://www.uscg.mil/HQ/MSC>. Owners or operators of foreign flag vessels that are subject to SOLAS Chapter XI must comply with this part by carrying on board a valid International Ship Security Certificate that certifies that the verifications required by Section 19.1 of part A of the ISPS Code (Incorporated by reference, see § 101.115 of this subchapter) have been completed. As stated in Section 9.4 of the ISPS Code, part A requires that, in order for the ISSC to be issued, the provisions of part B of the ISPS Code need to be taken into account.

(c) The VSP is sensitive security information and must be protected in accordance with 49 CFR part 1520.

(d) If the VSP is kept in an

electronic format, procedures must be in place to prevent its unauthorized deletion, destruction, or amendment.

§ 104.405 Format of the Vessel Security Plan (VSP).

(a) A vessel owner or operator must ensure that the VSP consists of the individual sections listed in this paragraph (a). If the VSP does not follow the order as it appears in the list, the vessel owner or operator must ensure that the VSP contains an index identifying the location of each of the following sections:

- (1) Security organization of the vessel;
- (2) Personnel training;
- (3) Drills and exercises;
- (4) Records and documentation;
- (5) Response to change in MARSEC Level;
- (6) Procedures for interfacing with facilities and other vessels;
- (7) Declarations of Security (DoS);
- (8) Communications;
- (9) Security systems and equipment maintenance;
- (10) Security measures for access control;
- (11) Security measures for restricted areas;
- (12) Security measures for handling cargo;
- (13) Security measures for delivery of vessel stores and bunkers;
- (14) Security measures for monitoring;
- (15) Security incident procedures;
- (16) Audits and Vessel Security Plan (VSP) amendments; and
- (17) Vessel Security Assessment (VSA) Report.

(b) The VSP must describe in detail how the requirements of subpart B of this part will be met.

§ 104.410 Submission and approval.

(a) In accordance with § 104.115, on or before December 31, 2003, each vessel owner or operator must either:

(1) Submit one copy of their Vessel Security Plan (VSP), in English, for review and approval to the

Commanding Officer, Marine Safety Center (MSC) and a letter certifying that the VSP meets applicable requirements of this part; or

(2) If intending to operate under an Approved Security Program, a letter signed by the vessel owner or operator stating which approved Alternative Security Program the owner or operator intends to use.

(b) Owners or operators of vessels not in service on or before December 31, 2003, must comply with the requirements in paragraph (a) of this section 60 days prior to beginning operations or by December 31, 2003, whichever is later.

(c) The Commanding Officer, Marine Safety Center (MSC), will examine each submission for compliance with this part, and either:

(1) Approve it and specify any conditions of approval, returning to the submitter a letter stating its acceptance and any conditions;

(2) Return it for revision, returning a copy to the submitter with brief descriptions of the required revisions; or

(3) Disapprove it, returning a copy to the submitter with a brief statement of the reasons for disapproval.

(d) A VSP may be submitted and approved to cover more than one vessel where the vessel design and operations are similar.

(e) Each company or vessel, owner or operator, that submits one VSP to cover two or more vessels of similar design and operation must address vessel-specific information that includes the physical and operational characteristics of each vessel.

(f) A plan that is approved by the MSC is valid for 5 years from the date of its approval.

§ 104.415 Amendment and audit.

(a) *Amendments.* (1) Amendments to a Vessel Security Plan that are approved by the Marine Safety Center (MSC) may be initiated by:

(i) The vessel owner or operator;

or
(ii) The Coast Guard upon a determination that an amendment is

needed to maintain the vessel's security. The Coast Guard will give the vessel owner or operator written notice and request that the vessel owner or operator propose amendments addressing any matters specified in the notice. The company owner or operator will have at least 60 days to submit its proposed amendments. Until amendments are approved, the company owner or operator shall ensure temporary security measures are implemented to the satisfaction of the Coast Guard.

(2) Proposed amendments must be sent to the MSC at the address shown in §104.400(b) of this part. If initiated by the company or vessel, owner or operator, the proposed amendment must be submitted at least 30 days before the amendment is to take effect unless the MSC allows a shorter period. The MSC will approve or disapprove the proposed amendment in accordance with §104.410 of this part.

(3) Nothing in this section should be construed as limiting the vessel owner or operator from the timely implementation of such additional security measures not enumerated in the approved VSP as necessary to address exigent security situations. In such cases, the owner or operator must notify the MSC by the most rapid means practicable as to the nature of the additional measures, the circumstances that prompted these additional measures, and the period of time these additional measures are expected to be in place.

(4) If the owner or operator has changed, the Vessel Security Officer (VSO) must amend the Vessel Security Plan (VSP) to include the name and contact information of the new vessel owner or operator and submit the affected portion of the VSP for review and approval in accordance with §104.410 of this part.

(b) *Audits.* (1) The CSO or VSO must ensure an audit of the VSP is performed annually, beginning no later than one year from the initial date of approval and attach a letter to the VSP certifying that the VSP meets the applicable requirements of this part.

(2) The VSP must be audited if there is a change in the company's or vessel's ownership or operator, or if

there have been modifications to the vessel, including but not limited to physical structure, emergency response procedures, security measures, or operations.

(3) Auditing the VSP as a result of modifications to the vessel may be limited to those sections of the VSP affected by the vessel modifications.

(4) Unless impracticable due to the size and nature of the company or the vessel, personnel conducting internal audits of the security measures specified in the VSP or evaluating its implementation must:

(i) Have knowledge of methods of conducting audits and inspections, and control and monitoring techniques;

(ii) Not have regularly assigned security duties; and

(iii) Be independent of any security measures being audited.

(5) If the results of an audit require amendment of either the VSA or VSP, the VSO or CSO must submit, in accordance with §104.410 of this part, the amendments to the MSC for review and approval no later than 30 days after completion of the audit and a letter certifying that the amended VSP meets the applicable requirements of this part.

33 CFR
Navigation and Navigable Waters
CHAPTER I
COAST GUARD, DEPARTMENT
OF HOMELAND SECURITY
SUBCHAPTER H -- MARITIME
SECURITY

PART 105—MARITIME
SECURITY: FACILITIES

Subpart A—General

Sec.

- 105.100 Definitions.
- 105.105 Applicability.
- 105.106 Public access areas.
- 105.110 Exemptions.
- 105.115 Compliance dates.
- 105.120 Compliance documentation.
- 105.125 Noncompliance.
- 105.130 Waivers.
- 105.135 Equivalents.
- 105.140 Alternative Security Program.
- 105.145 Maritime Security (MARSEC) Directive.
- 105.150 Right to appeal.

Subpart B -- Facility Security
Requirements

- 105.200 Owner or operator.
- 105.205 Facility Security Officer (FSO).
- 105.210 Facility personnel with security duties.
- 105.215 Security training for all other facility personnel.
- 105.220 Drill and exercise requirements.
- 105.225 Facility recordkeeping requirements.
- 105.230 Maritime Security (MARSEC) Level coordination and implementation.
- 105.235 Communications.
- 105.240 Procedures for interfacing with vessels.
- 105.245 Declaration of Security (DoS).
- 105.250 Security systems and equipment maintenance.
- 105.255 Security measures for access control.
- 105.260 Security measures for

- restricted areas.
- 105.265 Security measures for handling cargo.
- 105.270 Security measures for delivery of vessel stores and bunkers.
- 105.275 Security measures for monitoring.
- 105.280 Security incident procedures.
- 105.285 Additional requirements -- passenger and ferry facilities.
- 105.290 Additional requirements -- cruise ship terminals.
- 105.295 Additional requirements -- Certain Dangerous Cargo (CDC) facilities.
- 105.296 Additional requirements -- barge fleeting facilities.

Subpart C -- Facility Security
Assessment (FSA)

- 105.300 General.
- 105.305 Facility Security Assessment (FSA) requirements.
- 105.310 Submission requirements.

Subpart D -- Facility Security Plan
(FSP)

- 105.400 General.
- 105.405 Format and content of the Facility Security Plan (FSP).
- 105.410 Submission and approval.
- 105.415 Amendment and audit.
- Appendix A to part 105 -- Facility Vulnerability and Security Measure Summary (CG-6025).

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. 70103; 50 U.S.C. 191; 33 CFR 1.05–1, 6.04–11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No. 0170.1.

Source: USCG-2003-14732, 68 FR 39322, July 1, 2003, unless otherwise noted.

Subpart A—General

§ 105.100 Definitions.

Except as specifically stated in this subpart, the definitions in part 101 of this subchapter apply to this part.

§ 105.105 Applicability.

- (a) The requirements in this part

apply to the owner or operator of any U.S.:

(1) Facility subject to 33 CFR parts 126, 127, or 154;

(2) Facility that receives vessels certificated to carry more than 150 passengers, except those vessels not carrying and not embarking or disembarking passengers at the facility;

(3) Facility that receives vessels subject to the International Convention for Safety of Life at Sea, 1974, chapter XI;

(4) Facility that receives foreign cargo vessels greater than 100 gross register tons;

(5) Facility that receives U.S. cargo vessels, greater than 100 gross register tons, subject to 46 CFR chapter I, subchapter I, except for those facilities that receive only commercial fishing vessels inspected under 46 CFR part 105; or

(6) Barge fleeting facility that receives barges carrying, in bulk, cargoes regulated by 46 CFR chapter I, subchapters D or O, or Certain Dangerous Cargoes.

(b) An owner or operator of any facility not covered in paragraph (a) of this section is subject to parts 101 through 103 of this subchapter.

(c) This part does not apply to the owner or operator of the following U.S. facilities:

(1) A facility owned or operated by the U.S. that is used primarily for military purposes.

(2) An oil and natural gas production, exploration, or development facility regulated by 33 CFR parts 126 or 154 if:

(i) The facility is engaged solely in the exploration, development, or production of oil and natural gas; and

(ii) The facility does not meet or exceed the operating conditions in §106.105 of this subchapter;

(3) A facility that supports the production, exploration, or development of oil and natural gas regulated by 33 CFR parts 126 or 154 if:

(i) The facility is engaged solely in the support of exploration, development, or production of oil and natural gas and transports or stores quantities of hazardous materials that

do not meet or exceed those specified in 49 CFR 172.800(b)(1) through (b)(6); or

(ii) The facility stores less than 42,000 gallons of cargo regulated by 33 CFR part 154;

(4) A mobile facility regulated by 33 CFR part 154; or

(5) An isolated facility that receives materials regulated by 33 CFR parts 126 or 154 by vessel due to the lack of road access to the facility and does not distribute the material through secondary marine transfers.

§ 105.106 Public access areas.

(a) A facility serving ferries or passenger vessels certificated to carry more than 150 passengers, other than cruise ships, may designate an area within the facility as a public access area.

(b) A public access area is a defined space within a facility that is open to all persons and provides pedestrian access through the facility from public thoroughfares to the vessel.

§ 105.110 Exemptions.

(a) An owner or operator of any barge fleeting facility subject to this part is exempt from complying with §105.265, Security measures for handling cargo; and §105.270, Security measures for delivery of vessel stores and bunkers.

(b) A public access area designated under § 105.106 is exempt from the requirements for screening of persons, baggage, and personal effects and identification of persons in § 105.255(c), (e)(1), (e)(3), (f)(1), and (g)(1) and § 105.285(a)(1).

(c) An owner or operator of any general shipyard facility as defined in § 101.105 is exempt from the requirements of this part unless the facility:

(1) Is subject to parts 126, 127, or 154 of this chapter; or

(2) Provides any other service to vessels subject to part 104 of this subchapter not related to construction, repair, rehabilitation, refurbishment, or rebuilding.

(d) *Public access facility.* (1) The COTP may exempt a public access

facility from the requirements of this part, including establishing conditions for which such an exemption is granted, to ensure that adequate security is maintained.

(2) The owner or operator of any public access facility exempted under this section must:

(i) Comply with any COTP conditions for the exemption; and

(ii) Ensure that the cognizant COTP has the appropriate information for contacting the individual with security responsibilities for the public access facility at all times.

(3) The cognizant COTP may withdraw the exemption for a public access facility at any time the owner or operator fails to comply with any requirement of the COTP as a condition of the exemption or any measure ordered by the COTP pursuant to existing COTP authority.

(e) An owner or operator of a facility is not subject to this part if the facility receives only vessels to be laid-up, dismantled, or otherwise placed out of commission provided that the vessels are not carrying and do not receive cargo or passengers at that facility.

§ 105.115 Compliance dates.

(a) On or before December 31, 2003, facility owners or operators must submit to the cognizant COTP for each facility—

(1) The Facility Security Plan described in subpart D of this part for review and approval; or

(2) If intending to operate under an approved Alternative Security Program, a letter signed by the facility owner or operator stating which approved Alternative Security Program the owner or operator intends to use.

(b) On or before July 1, 2004, each facility owner or operator must be operating in compliance with this part.

§ 105.120 Compliance documentation.

Each facility owner or operator subject to this part must ensure, on or before July 1, 2004, that copies of the following documentation are available at the facility and are made available to the Coast Guard upon request:

(a) The approved Facility Security Plan (FSP), as well as any approved revisions or amendments thereto, and a letter of approval from the COTP dated within the last 5 years;

(b) The FSP submitted for approval and an acknowledgement letter from the COTP stating that the Coast Guard is currently reviewing the FSP submitted for approval, and that the facility may continue to operate so long as the facility remains in compliance with the submitted FSP; or

(c) For facilities operating under a Coast Guard-approved Alternative Security Program as provided in §105.140, a copy of the Alternative Security Program the facility is using, including a facility specific security assessment report generated under the Alternative Security Program, as specified in § 101.120(b)(3) of this subchapter, and a letter signed by the facility owner or operator, stating which Alternative Security Program the facility is using and certifying that the facility is in full compliance with that program.

§ 105.125 Noncompliance.

When a facility must temporarily deviate from the requirements of this part, the facility owner or operator must notify the cognizant COTP, and either suspend operations or request and receive permission from the COTP to continue operating.

§ 105.130 Waivers.

Any facility owner or operator may apply for a waiver of any requirement of this part that the facility owner or operator considers unnecessary in light of the nature or operating conditions of the facility, prior to operating. A request for a waiver must be submitted in writing with justification to the Commandant (G-MP) at 2100 Second St., SW., Washington, DC 20593. The Commandant (G-MP) may require the facility owner or operator to provide data for use in determining the validity of the requested waiver. The Commandant (G-MP) may grant, in writing, a waiver with or without conditions only if the waiver will not reduce the overall security of the

facility, its employees, visiting vessels, or ports.

[USCG–2003–14732, 68 FR 39322, July 1, 2003; 68 FR 41916, July 16, 2003]

§ 105.135 Equivalents.

For any measure required by this part, the facility owner or operator may propose an equivalent as provided in §101.130 of this subchapter.

§ 105.140 Alternative Security Program.

(a) A facility owner or operator may use an Alternative Security Program approved under §101.120 of this subchapter if:

(1) The Alternative Security Program is appropriate to that facility;

(2) The Alternative Security Program is implemented in its entirety.

(b) A facility owner or operator using an Alternative Security Program approved under §101.120 of this subchapter must complete and submit to the cognizant COTP a Facility Vulnerability and Security Measures Summary (Form CG–6025) in appendix A to part 105—Facility Vulnerability and Security (CG–6025).

§ 105.145 Maritime Security (MARSEC) Directive.

Each facility owner or operator subject to this part must comply with any instructions contained in a MARSEC Directive issued under §101.405 of this subchapter.

§ 105.150 Right to appeal.

Any person directly affected by a decision or action taken under this part, by or on behalf of the Coast Guard, may appeal as described in §101.420 of this subchapter.

Subpart B—Facility Security Requirements

§ 105.200 Owner or operator.

(a) Each facility owner or operator must ensure that the facility operates in compliance with the

requirements of this part.

(b) For each facility, the facility owner or operator must:

(1) Define the security organizational structure and provide each person exercising security duties and responsibilities within that structure the support needed to fulfill those obligations;

(2) Designate, in writing, by name or by title, a Facility Security Officer (FSO) and identify how the officer can be contacted at any time;

(3) Ensure that a Facility Security Assessment (FSA) is conducted;

(4) Ensure the development and submission for approval of a Facility Security Plan (FSP);

(5) Ensure that the facility operates in compliance with the approved FSP;

(6) Ensure that adequate coordination of security issues takes place between the facility and vessels that call on it, including the execution of a Declaration of Security (DoS) as required by this part;

(7) Ensure coordination of shore leave for vessel personnel or crew change-out, as well as access through the facility for visitors to the vessel (including representatives of seafarers' welfare and labor organizations), with vessel operators in advance of a vessel's arrival. In coordinating such leave, facility owners or operators may refer to treaties of friendship, commerce, and navigation between the U.S. and other nations. The text of these treaties can be found on the U.S. Department of State's website at <http://www.state.gov/s/l/24224.htm>;

(8) Ensure, within 12 hours of notification of an increase in MARSEC Level, implementation of the additional security measures required for the new MARSEC Level;

(9) Ensure security for unattended vessels moored at the facility;

(10) Ensure the report of all breaches of security and transportation security incidents to the National Response Center in accordance with part 101 of this chapter; and

(11) Ensure consistency between security requirements and safety

requirements.

§ 105.205 Facility Security Officer (FSO).

(a) *General.* (1) The FSO may perform other duties within the owner's or operator's organization, provided he or she is able to perform the duties and responsibilities required of the FSO.

(2) The same person may serve as the FSO for more than one facility, provided the facilities are in the same COTP zone and are not more than 50 miles apart. If a person serves as the FSO for more than one facility, the name of each facility for which he or she is the FSO must be listed in the Facility Security Plan (FSP) of each facility for which or she is the FSO.

(3) The FSO may assign security duties to other facility personnel; however, the FSO retains the responsibility for these duties.

(b) *Qualifications.* (1) The FSO must have general knowledge, through training or equivalent job experience, in the following:

(i) Security organization of the facility;

(ii) General vessel and facility operations and conditions;

(iii) Vessel and facility security measures, including the meaning and the requirements of the different MARSEC Levels;

(iv) Emergency preparedness, response, and contingency planning;

(v) Security equipment and systems, and their operational limitations; and

(vi) Methods of conducting audits, inspections, control, and monitoring techniques.

(2) In addition to knowledge and training required in paragraph (b)(1) of this section, the FSO must have knowledge of and receive training in the following, as appropriate:

(i) Relevant international laws and codes, and recommendations;

(ii) Relevant government legislation and regulations;

(iii) Responsibilities and functions of local, State, and Federal law enforcement agencies;

(iv) Security assessment methodology;

(v) Methods of facility security surveys and inspections;

(vi) Instruction techniques for security training and education, including security measures and procedures;

(vii) Handling sensitive security information and security related communications;

(viii) Current security threats and patterns;

(ix) Recognizing and detecting dangerous substances and devices;

(x) Recognizing characteristics and behavioral patterns of persons who are likely to threaten security;

(xi) Techniques used to circumvent security measures;

(xii) Conducting physical searches and non-intrusive inspections;

(xiii) Conducting security drills and exercises, including exercises with vessels; and

(xiv) Assessing security drills and exercises.

(c) *Responsibilities.* In addition to those responsibilities and duties specified elsewhere in this part, the FSO must, for each facility for which he or she has been designated:

(1) Ensure that the Facility Security Assessment (FSA) is conducted;

(2) Ensure the development and implementation of a FSP;

(3) Ensure that an annual audit is conducted, and if necessary that the FSA and FSP are updated;

(4) Ensure the FSP is exercised per §105.220 of this part;

(5) Ensure that regular security inspections of the facility are conducted;

(6) Ensure the security awareness and vigilance of the facility personnel;

(7) Ensure adequate training to personnel performing facility security duties;

(8) Ensure that occurrences that threaten the security of the facility are recorded and reported to the owner or operator;

(9) Ensure the maintenance of records required by this part;

(10) Ensure the preparation and the submission of any reports as required by this part;

(11) Ensure the execution of any required Declarations of Security with Masters, Vessel Security Officers or their designated representatives;

(12) Ensure the coordination of security services in accordance with the approved FSP;

(13) Ensure that security equipment is properly operated, tested, calibrated, and maintained;

(14) Ensure the recording and reporting of attainment changes in MARSEC Levels to the owner or operator and the cognizant COTP;

(15) When requested, ensure that the Vessel Security Officers receive assistance in confirming the identity of visitors and service providers seeking to board the vessel through the facility;

(16) Ensure notification, as soon as possible, to law enforcement personnel and other emergency responders to permit a timely response to any transportation security incident;

(17) Ensure that the FSP is submitted to the cognizant COTP for approval, as well as any plans to change the facility or facility infrastructure prior to amending the FSP; and

(18) Ensure that all facility personnel are briefed of changes in security conditions at the facility.

§ 105.210 Facility personnel with security duties.

Facility personnel responsible for security duties must have knowledge, through training or equivalent job experience, in the following, as appropriate:

(a) Knowledge of current security threats and patterns;

(b) Recognition and detection of dangerous substances and devices;

(c) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

(d) Techniques used to circumvent security measures;

(e) Crowd management and control techniques;

(f) Security related communications;

(g) Knowledge of emergency procedures and contingency plans;

(h) Operation of security

equipment and systems;

(i) Testing, calibration, and maintenance of security equipment and systems;

(j) Inspection, control, and monitoring techniques;

(k) Relevant provisions of the Facility Security Plan (FSP);

(l) Methods of physical screening of persons, personal effects, baggage, cargo, and vessel stores; and

(m) The meaning and the consequential requirements of the different MARSEC Levels.

§ 105.215 Security training for all other facility personnel.

All other facility personnel, including contractors, whether part-time, full-time, temporary, or permanent, must have knowledge of, through training or equivalent job experience, in the following, as appropriate:

(a) Relevant provisions of the Facility Security Plan (FSP);

(b) The meaning and the consequential requirements of the different MARSEC Levels as they apply to them, including emergency procedures and contingency plans;

(c) Recognition and detection of dangerous substances and devices;

(d) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security; and

(e) Techniques used to circumvent security measures.

§ 105.220 Drill and exercise requirements.

(a) *General.* (1) Drills and exercises must test the proficiency of facility personnel in assigned security duties at all MARSEC Levels and the effective implementation of the Facility Security Plan (FSP). They must enable the Facility Security Officer (FSO) to identify any related security deficiencies that need to be addressed.

(2) A drill or exercise required by this section may be satisfied with the implementation of security measures required by the FSP as the result of an increase in the MARSEC Level, provided the facility reports attainment

to the cognizant COTP.

(b) *Drills.* (1) The FSO must ensure that at least one security drill is conducted every 3 months. Security drills may be held in conjunction with non-security drills, where appropriate.

(2) Drills must test individual elements of the FSP, including response to security threats and incidents. Drills should take into account the types of operations of the facility, facility personnel changes, the type of vessel the facility is serving, and other relevant circumstances. Examples of drills include unauthorized entry to a restricted area, response to alarms, and notification of law enforcement authorities.

(3) If a vessel is moored at the facility on the date the facility has planned to conduct any drills, the facility cannot require the vessel or vessel personnel to be a part of or participate in the facility's scheduled drill.

(c) *Exercises.* (1) Exercises must be conducted at least once each calendar year, with no more than 18 months between exercises.

(2) Exercises may be:

- (i) Full scale or live;
- (ii) Tabletop simulation or seminar;
- (iii) Combined with other appropriate exercises; or
- (iv) A combination of the elements in paragraphs (c)(2)(i) through (iii) of this section.

(3) Exercises may be facility-specific or part of a cooperative exercise program with applicable facility and vessel security plans or comprehensive port exercises.

(4) Each exercise must test communication and notification procedures, and elements of coordination, resource availability, and response.

(5) Exercises are a full test of the security program and must include substantial and active participation of FSOs, and may include government authorities and vessels visiting the facility. Requests for participation of Company and Vessel Security Officers in joint exercises should consider the security and work implications for the vessel.

§ 105.225 Facility recordkeeping requirements.

(a) Unless otherwise specified in this section, the Facility Security Officer (FSO) must keep records of the activities as set out in paragraph (b) of this section for at least 2 years and make them available to the Coast Guard upon request.

(b) Records required by this section may be kept in electronic format. If kept in an electronic format, they must be protected against unauthorized deletion, destruction, or amendment. The following records must be kept:

(1) *Training.* For training under § 105.210, the date of each session, duration of session, a description of the training, and a list of attendees;

(2) *Drills and exercises.* For each drill or exercise, the date held, description of drill or exercise, list of participants, and any best practices or lessons learned which may improve the Facility Security Plan (FSP);

(3) *Incidents and breaches of security.* For each incident or breach of security, the date and time of occurrence, location within the facility, description of incident or breaches, to whom it was reported, and description of the response;

(4) *Changes in MARSEC Levels.* For each change in MARSEC Level, the date and time of notification received, and time of compliance with additional requirements;

(5) *Maintenance, calibration, and testing of security equipment.* For each occurrence of maintenance, calibration, and testing, record the date and time, and the specific security equipment involved;

(6) *Security threats.* For each security threat, the date and time of occurrence, how the threat was communicated, who received or identified the threat, description of threat, to whom it was reported, and description of the response;

(7) *Declaration of Security (DoS).* A copy of each single-visit DoS and a copy of each continuing DoS for at least 90 days after the end of its effective period; and

(8) *Annual audit of the FSP.* For

each annual audit, a letter certified by the FSO stating the date the audit was completed.

(c) Any record required by this part must be protected from unauthorized access or disclosure.

§ 105.230 Maritime Security (MARSEC) Level coordination and implementation.

(a) The facility owner or operator must ensure the facility operates in compliance with the security requirements in this part for the MARSEC Level in effect for the port.

(b) When notified of an increase in the MARSEC Level, the facility owner and operator must ensure:

(1) Vessels moored to the facility and vessels scheduled to arrive at the facility within 96 hours of the MARSEC Level change are notified of the new MARSEC Level and the Declaration of Security is revised as necessary;

(2) The facility complies with the required additional security measures within 12 hours; and

(3) The facility reports compliance or noncompliance to the COTP.

(c) For MARSEC Levels 2 and 3, the Facility Security Officer must inform all facility personnel about identified threats, and emphasize reporting procedures and stress the need for increased vigilance.

(d) An owner or operator whose facility is not in compliance with the requirements of this section, must inform the COTP and obtain approval prior to interfacing with a vessel or continuing operations.

(e) At MARSEC Level 3, in addition to the requirements in this part, a facility owner or operator may be required to implement additional measures, pursuant to 33 CFR part 6, 160, or 165, as appropriate, which may include but are not limited to:

(1) Use of waterborne security patrol;

(2) Use of armed security personnel to control access to the facility and to deter, to the maximum extent practical, a transportation security incident; and

(3) Examination of piers, wharves, and similar structures at the facility for the presence of dangerous substances or devices underwater or other threats.

§ 105.235 Communications.

(a) The Facility Security Officer must have a means to effectively notify facility personnel of changes in security conditions at the facility.

(b) Communication systems and procedures must allow effective and continuous communications between the facility security personnel, vessels interfacing with the facility, the cognizant COTP, and national and local authorities with security responsibilities.

(c) At each active facility access point, provide a means of contacting police, security control, or an emergency operations center, by telephones, cellular phones, and/or portable radios, or other equivalent means.

(d) Facility communications systems must have a backup means for both internal and external communications.

§ 105.240 Procedures for interfacing with vessels.

The facility owner or operator must ensure that there are measures for interfacing with vessels at all MARSEC Levels.

§ 105.245 Declaration of Security (DoS).

(a) Each facility owner or operator must ensure procedures are established for requesting a DoS and for handling DoS requests from a vessel.

(b) At MARSEC Level 1, a facility receiving a cruise ship or a manned vessel carrying Certain Dangerous Cargo, in bulk, must comply with the following:

(1) Prior to the arrival of a vessel to the facility, the Facility Security Officer (FSO) and Master, Vessel Security Officer (VSO), or their designated representatives must coordinate security needs and procedures, and agree upon the contents

of the DoS for the period of time the vessel is at the facility; and

(2) Upon the arrival of the vessel at the facility, the FSO and Master, VSO, or their designated representative, must sign the written DoS.

(c) Neither the facility nor the vessel may embark or disembark passengers, nor transfer cargo or vessel stores until the DoS has been signed and implemented.

(d) At MARSEC Levels 2 and 3, the FSOs, or their designated representatives, of facilities interfacing with manned vessels subject to part 104, of this subchapter must sign and implement DoSs as required in (b)(1) and (2) of this section.

(e) At MARSEC Levels 1 and 2, FSOs of facilities that frequently interface with the same vessel may implement a continuing DoS for multiple visits, provided that:

(1) The DoS is valid for a specific MARSEC Level;

(2) The effective period at MARSEC Level 1 does not exceed 90 days; and

(3) The effective period at MARSEC Level 2 does not exceed 30 days.

(f) When the MARSEC Level increases beyond that contained in the DoS, the continuing DoS is void and a new DoS must be executed in accordance with this section.

(g) A copy of all currently valid continuing DoSs must be kept with the Facility Security Plan.

(h) The COTP may require, at any time, at any MARSEC Level, any facility subject to this part to implement a DoS with the VSO prior to any vessel-to-facility interface when he or she deems it necessary.

§ 105.250 Security systems and equipment maintenance.

(a) Security systems and equipment must be in good working order and inspected, tested, calibrated, and maintained according to manufacturers' recommendations.

(b) Security systems must be regularly tested in accordance with the manufacturers' recommendations; noted deficiencies corrected promptly;

and the results recorded as required in §105.225 of this subpart.

(c) The FSP must include procedures for identifying and responding to security system and equipment failures or malfunctions.

§ 105.255 Security measures for access control.

(a) *General.* The facility owner or operator must ensure the implementation of security measures to:

(1) Deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, facilities, or ports;

(2) Secure dangerous substances and devices that are authorized by the owner or operator to be on the facility; and

(3) Control access to the facility.

(b) The facility owner or operator must ensure that the following are specified:

(1) The locations where restrictions or prohibitions that prevent unauthorized access are applied for each MARSEC Level. Each location allowing means of access to the facility must be addressed;

(2) The identification of the type of restriction or prohibition to be applied and the means of enforcing them;

(3) The means of identification required to allow access to the facility and for individuals and vehicles to remain on the facility without challenge; and

(4) The identification of the locations where persons, personal effects and vehicle screenings are to be conducted. The designated screening areas should be covered to provide for continuous operations regardless of the weather conditions.

(c) The facility owner or operator must ensure that an identification system is established for checking the identification of facility personnel or other persons seeking access to the facility that:

(1) Allows identification of authorized and unauthorized persons at any MARSEC Level;

(2) Is coordinated, when

practicable, with identification systems of vessels or other transportation conveyances that use the facility;

(3) Is updated regularly;

(4) Uses disciplinary measures to discourage abuse;

(5) Allows temporary or continuing access for facility personnel and visitors, including seafarers' chaplains and union representatives, through the use of a badge or other system to verify their identity; and

(6) Allows certain long-term, frequent vendor representatives to be treated more as employees than as visitors.

(d) The facility owner or operator must establish in the approved Facility Security Plan (FSP) the frequency of application of any access controls, particularly if they are to be applied on a random or occasional basis.

(e) *MARSEC Level 1*. The facility owner or operator must ensure the following security measures are implemented at the facility:

(1) Screen persons, baggage (including carry-on items), personal effects, and vehicles, for dangerous substances and devices at the rate specified in the approved FSP, excluding government-owned vehicles on official business when government personnel present identification credentials for entry;

(2) Conspicuously post signs that describe security measures currently in effect and clearly state that:

(i) Entering the facility is deemed valid consent to screening or inspection; and

(ii) Failure to consent or submit to screening or inspection will result in denial or revocation of authorization to enter;

(3) Check the identification of any person seeking to enter the facility, including vessel passengers and crew, facility employees, vendors, personnel duly authorized by the cognizant authority, and visitors. This check includes confirming the reason for entry by examining at least one of the following:

(i) Joining instructions;

(ii) Passenger tickets;

(iii) Boarding passes;

(iv) Work orders, pilot orders, or surveyor orders;

(v) Government identification; or

(vi) Visitor badges issued in accordance with an identification system required in paragraph (c) of this section;

(4) Deny or revoke a person's authorization to be on the facility if the person is unable or unwilling, upon the request of facility personnel, to establish his or her identity or to account for his or her presence. Any such incident must be reported in compliance with this part;

(5) Designate restricted areas and provide appropriate access controls for these areas;

(6) Identify access points that must be secured or attended to deter unauthorized access;

(7) Deter unauthorized access to the facility and to designated restricted areas within the facility;

(8) Screen by hand or device, such as x-ray, all unaccompanied baggage prior to loading onto a vessel; and

(9) Secure unaccompanied baggage after screening in a designated restricted area and maintain security control during transfers between the facility and a vessel.

(f) *MARSEC Level 2*. In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in their approved FSP. These additional security measures may include:

(1) Increasing the frequency and detail of the screening of persons, baggage, and personal effects for dangerous substances and devices entering the facility;

(2) X-ray screening of all unaccompanied baggage;

(3) Assigning additional personnel to guard access points and patrol the perimeter of the facility to deter unauthorized access;

(4) Limiting the number of access points to the facility by closing and securing some access points and providing physical barriers to impede

movement through the remaining access points;

(5) Denying access to visitors who do not have a verified destination;

(6) Deterring waterside access to the facility, which may include, using waterborne patrols to enhance security around the facility; or

(7) Except for government-owned vehicles on official business when government personnel present identification credentials for entry, screening vehicles and their contents for dangerous substances and devices at the rate specified for MARSEC Level 2 in the approved FSP.

(g) *MARSEC Level 3.* In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, the facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in their approved FSP. These additional security measures may include:

(1) Screening all persons, baggage, and personal effects for dangerous substances and devices;

(2) Performing one or more of the following on unaccompanied baggage:

(i) Screen unaccompanied baggage more extensively; for example, x-raying from two or more angles;

(ii) Prepare to restrict or suspend handling unaccompanied baggage; or

(iii) Refuse to accept unaccompanied baggage;

(3) Being prepared to cooperate with responders and facilities;

(4) Granting access to only those responding to the security incident or threat thereof;

(5) Suspending access to the facility;

(6) Suspending cargo operations;

(7) Evacuating the facility;

(8) Restricting pedestrian or vehicular movement on the grounds of the facility; or

(9) Increasing security patrols within the facility.

§ 105.260 Security measures for restricted areas.

(a) *General.* The facility owner

or operator must ensure the designation of restricted areas in order to:

(1) Prevent or deter unauthorized access;

(2) Protect persons authorized to be in the facility;

(3) Protect the facility;

(4) Protect vessels using and serving the facility;

(5) Protect sensitive security areas within the facility;

(6) Protect security and surveillance equipment and systems; and

(7) Protect cargo and vessel stores from tampering.

(b) *Designation of Restricted Areas.* The facility owner or operator must ensure restricted areas are designated within the facility. They must also ensure that all restricted areas are clearly marked and indicate that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security. The facility owner or operator may also designate the entire facility as a restricted area. Restricted areas must include, as appropriate:

(1) Shore areas immediately adjacent to each vessel moored at the facility;

(2) Areas containing sensitive security information, including cargo documentation;

(3) Areas containing security and surveillance equipment and systems and their controls, and lighting system controls; and

(4) Areas containing critical facility infrastructure, including:

(i) Water supplies;

(ii) Telecommunications;

(iii) Electrical system; and

(iv) Access points for ventilation and air-conditioning systems;

(5) Manufacturing or processing areas and control rooms;

(6) Locations in the facility where access by vehicles and personnel should be restricted;

(7) Areas designated for loading, unloading or storage of cargo and stores; and

(8) Areas containing cargo consisting of dangerous goods or hazardous substances, including certain dangerous cargoes.

(c) The owner or operator must ensure that all restricted areas have clearly established security measures to:

(1) Identify which facility personnel are authorized to have access;

(2) Determine which persons other than facility personnel are authorized to have access;

(3) Determine the conditions under which that access may take place;

(4) Define the extent of any restricted area;

(5) Define the times when access restrictions apply;

(6) Clearly mark all restricted areas and indicate that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security;

(7) Control the entry, parking, loading and unloading of vehicles;

(8) Control the movement and storage of cargo and vessel stores; and

(9) Control unaccompanied baggage or personal effects.

(d) *MARSEC Level 1.* At MARSEC Level 1, the facility owner or operator must ensure the implementation of security measures to prevent unauthorized access or activities within the area. These security measures may include:

(1) Restricting access to only authorized personnel;

(2) Securing all access points not actively used and providing physical barriers to impede movement through the remaining access points;

(3) Assigning personnel to control access to restricted areas;

(4) Verifying the identification and authorization of all persons and all vehicles seeking entry;

(5) Patrolling or monitoring the perimeter of restricted areas;

(6) Using security personnel, automatic intrusion detection devices, surveillance equipment, or surveillance systems to detect unauthorized entry or movement within restricted areas;

(7) Directing the parking, loading, and unloading of vehicles within a restricted area;

(8) Controlling unaccompanied baggage and or personal effects after screening;

(9) Designating restricted areas for performing inspections of cargo and

vessel stores while awaiting loading; and

(10) Designating temporary restricted areas to accommodate facility operations. If temporary restricted areas are designated, the FSP must include a requirement to conduct a security sweep of the designated temporary restricted area both before and after the area has been established.

(e) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in their approved FSP. These additional security measures may include:

(1) Increasing the intensity and frequency of monitoring and access controls on existing restricted access areas;

(2) Enhancing the effectiveness of the barriers or fencing surrounding restricted areas, by the use of patrols or automatic intrusion detection devices;

(3) Reducing the number of access points to restricted areas, and enhancing the controls applied at the remaining accesses;

(4) Restricting parking adjacent to vessels;

(5) Further restricting access to the restricted areas and movements and storage within them;

(6) Using continuously monitored and recorded surveillance equipment;

(7) Enhancing the number and frequency of patrols, including waterborne patrols undertaken on the boundaries of the restricted areas and within the areas; or

(8) Establishing and restricting access to areas adjacent to the restricted areas.

(f) *MARSEC Level 3.* In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in their approved FSP. These additional security measures may include:

(1) Restricting access to additional areas;

(2) Prohibiting access to restricted areas, or

(3) Searching restricted areas as part of a security sweep of all or part of the facility.

§ 105.265 Security measures for handling cargo.

(a) *General.* The facility owner or operator must ensure that security measures relating to cargo handling, some of which may have to be applied in liaison with the vessel, are implemented in order to:

(1) Deter tampering;

(2) Prevent cargo that is not meant for carriage from being accepted and stored at the facility without the knowing consent of the facility owner or operator;

(3) Identify cargo that is approved for loading onto vessels interfacing with the facility;

(4) Include cargo control procedures at access points to the facility;

(5) Identify cargo that is accepted for temporary storage in a restricted area while awaiting loading or pick up;

(6) Restrict the entry of cargo to the facility that does not have a confirmed date for loading, as appropriate;

(7) Ensure the release of cargo only to the carrier specified in the cargo documentation;

(8) When there are regular or repeated cargo operations with the same shipper, coordinate security measures with the shipper or other responsible party in accordance with an established agreement and procedure; and

(9) Create, update, and maintain a continuous inventory of all dangerous goods and hazardous substances from receipt to delivery within the facility, giving the location of those dangerous goods and hazardous substances.

(b) *MARSEC Level 1.* At MARSEC Level 1, the facility owner or operator must ensure the implementation of measures to:

(1) Unless unsafe to do so, routinely check cargo, cargo transport

units, and cargo storage areas within the facility prior to, and during, cargo handling operations for evidence of tampering;

(2) Check that cargo, containers, or other cargo transport units entering the facility match the delivery note or equivalent cargo documentation;

(3) Screen vehicles; and

(4) Check seals and other methods used to prevent tampering upon entering the facility and upon storage within the facility.

(c) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved FSP. These additional security measures may include:

(1) Conducting check of cargo, containers or other cargo transport units, and cargo storage areas within the facility for evidence of tampering;

(2) Intensifying checks, as appropriate, to ensure that only the documented cargo enters the facility, is temporarily stored there, and then loaded onto the vessel;

(3) Intensifying the screening of vehicles;

(4) Increasing frequency and detail in checking of seals and other methods used to prevent tampering;

(5) Coordinating enhanced security measures with the shipper or other responsible party in accordance with an established agreement and procedures;

(6) Increasing the frequency and intensity of visual and physical inspections; or

(7) Limiting the number of locations where dangerous goods and hazardous substances, including certain dangerous cargoes, can be stored.

(d) *MARSEC Level 3.* In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved FSP. These additional security measures may

include:

- (1) Restricting or suspending cargo movements or operations within all or part of the facility or specific vessels;
- (2) Being prepared to cooperate with responders and vessels; or
- (3) Verifying the inventory and location of any dangerous goods and hazardous substances, including certain dangerous cargoes, held within the facility and their location.

§ 105.270 Security measures for delivery of vessel stores and bunkers.

(a) *General.* The facility owner or operator must ensure that security measures relating to the delivery of vessel stores and bunkers are implemented to:

- (1) Check vessel stores for package integrity;
- (2) Prevent vessel stores from being accepted without inspection;
- (3) Deter tampering;
- (4) For vessels that routinely use a facility, establish and execute standing arrangements between the vessel, its suppliers, and a facility regarding notification and the timing of deliveries and their documentation; and
- (5) Check vessel stores by the following means:
 - (i) Visual examination;
 - (ii) Physical examination;
 - (iii) Detection devices, such as scanners; or
 - (iv) Canines.

(b) *MARSEC Level 1.* At MARSEC Level 1, the facility owner or operator must ensure the implementation of measures to:

- (1) Screen vessel stores at the rate specified in the approved Facility Security Plan (FSP);
- (2) Require advance notification of vessel stores or bunkers delivery, including a list of stores, delivery vehicle driver information, and vehicle registration information;
- (3) Screen delivery vehicles at the frequencies specified in the approved FSP; and
- (4) Escort delivery vehicles within the facility at the rate specified by the approved FSP.

(c) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved FSP. These additional security measures may include:

- (1) Detailed screening of vessel stores;
- (2) Detailed screening of all delivery vehicles;
- (3) Coordinating with vessel personnel to check the order against the delivery note prior to entry to the facility;
- (4) Ensuring delivery vehicles are escorted within the facility; or
- (5) Restricting or prohibiting the entry of vessel stores that will not leave the facility within a specified period.

(d) *MARSEC Level 3.* In addition to the security measures for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the facility owner and operator must ensure implementation of additional security measures, as specified for MARSEC Level 3 in the approved FSP. Examples of these additional security measures may include:

- (1) Checking all vessel stores more extensively;
- (2) Restricting or suspending delivery of vessel stores; or
- (3) Refusing to accept vessel stores on the facility.

§ 105.275 Security measures for monitoring.

(a) *General.* The facility owner or operator must ensure the implementation of security measures in this section and have the capability to continuously monitor, through a combination of lighting, security guards, waterborne patrols, automatic intrusion-detection devices, or surveillance equipment, as specified in the approved Facility Security Plan (FSP), the:

- (1) Facility and its approaches, on land and water;
- (2) Restricted areas within the facility; and

(3) Vessels at the facility and areas surrounding the vessels.

(b) *MARSEC Level 1.* At MARSEC Level 1, the facility owner or operator must ensure the security measures in this section are implemented at all times, including the period from sunset to sunrise and periods of limited visibility. For each facility, ensure monitoring capability that:

(1) When automatic intrusion-detection devices are used, activates an audible or visual alarm, or both, at a location that is continuously attended or monitored;

(2) Is able to function continually, including consideration of the possible effects of weather or of a power disruption;

(3) Monitors the facility area, including shore and waterside access to it;

(4) Monitors access points, barriers and restricted areas;

(5) Monitors access and movements adjacent to vessels using the facility, including augmentation of lighting provided by the vessel itself; and

(6) Limits lighting effects, such as glare, and their impact on safety, navigation, and other security activities.

(c) *MARSEC Level 2.* In addition to the security measures for MARSEC Level 1 in this section, at MARSEC Level 2, the facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved FSP. These additional measures may include:

(1) Increasing the coverage and intensity of surveillance equipment, including the provision of additional surveillance coverage;

(2) Increasing the frequency of foot, vehicle or waterborne patrols;

(3) Assigning additional security personnel to monitor and patrol; or

(4) Increasing the coverage and intensity of lighting, including the provision of additional lighting and coverage.

(d) *MARSEC Level 3.* In addition to the security measures for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the facility owner

or operator must also ensure implementation of additional security measures, as specified for MARSEC Level 3 in the approved FSP. These additional security measures may include:

(1) Switching on all lighting within, or illuminating the vicinity of, the facility;

(2) Switching on all surveillance equipment capable of recording activities within or adjacent to the facility;

(3) Maximizing the length of time such surveillance equipment can continue to record; or

(4) Complying with the instructions issued by those responding to the security incident.

§ 105.280 Security incident procedures.

For each MARSEC Level, the facility owner or operator must ensure the Facility Security Officer and facility security personnel are able to:

(a) Respond to security threats or breaches of security and maintain critical facility and vessel-to-facility interface operations;

(b) Evacuate the facility in case of security threats or breaches of security;

(c) Report security incidents as required in §101.305 of this subchapter;

(d) Brief all facility personnel on possible threats and the need for vigilance, soliciting their assistance in reporting suspicious persons, objects, or activities; and

(e) Secure non-critical operations in order to focus response on critical operations.

§ 105.285 Additional requirements-passenger and ferry facilities.

(a) At all MARSEC Levels, the owner or operator of a passenger or ferry facility must ensure, in coordination with a vessel moored at the facility, that the following security measures are implemented in addition to the requirements of this part:

(1) Establish separate areas to segregate unchecked persons and personal effects from checked persons

and personal effects;

(2) Ensure that a defined percentage of vehicles to be loaded aboard are screened prior to loading, in accordance with a MARSEC Directive or other orders issued by the Coast Guard;

(3) Ensure that all unaccompanied vehicles to be loaded on passenger vessels are screened prior to loading;

(4) Deny passenger access to restricted areas unless supervised by facility security personnel; and

(5) In a facility with a public access area designated under § 105.106, provide sufficient security personnel to monitor all persons within the area.

(b) At MARSEC Level 2, in addition to the requirements in paragraph (a) of this section, the owner or operator of a passenger or ferry facility with a public access area designated under § 105.106 must increase the intensity of monitoring of the public access area.

(c) At MARSEC Level 3, in addition to the requirements in paragraph (a) of this section, the owner or operator of a passenger or ferry facility with a public access area designated under § 105.106 must increase the intensity of monitoring and assign additional security personnel to monitor the public access area.

§ 105.290 Additional requirements—cruise ship terminals.

At all MARSEC Levels, in coordination with a vessel moored at the facility, the facility owner or operator must ensure the following security measures:

(a) Screen all persons, baggage, and personal effects for dangerous substances and devices;

(b) Check the identification of all persons seeking to board the vessel. This includes confirming the reason for boarding by examining joining instructions, passenger tickets, boarding passes, government identification or visitor badges, or work orders;

(c) Designate holding, waiting, or embarkation areas to segregate screened persons and their personal effects awaiting embarkation from

unscreened persons and their personal effects;

(d) Provide additional security personnel to designated holding, waiting, or embarkation areas; and

(e) Deny passenger access to restricted areas unless supervised by facility security personnel.

§ 105.295 Additional requirements—Certain Dangerous Cargo (CDC) facilities.

(a) At all MARSEC Levels, owners or operators of CDC facilities must ensure the implementation of the following security measures in addition to the requirements of this part:

(1) Escort all visitors, contractors, vendors, and other non-facility employees at all times while on the facility, if access identification is not provided. Escort provisions do not apply to prearranged cargo deliveries;

(2) Control the parking, loading, and unloading of vehicles within a facility;

(3) Require security personnel to record or report their presence at key points during their patrols;

(4) Search unmanned or unmonitored waterfront areas for dangerous substances and devices prior to a vessel's arrival at the facility; and

(5) Provide an alternate or independent power source for security and communications systems.

(b) At MARSEC Level 2, in addition to the requirements for MARSEC Level 1, owners or operators of CDC facilities must ensure the implementation of the following security measures:

(1) Release cargo only in the presence of the Facility Security Officer (FSO) or a designated representative of the FSO; and

(2) Continuously patrol restricted areas.

(c) At MARSEC Level 3, in addition to the requirements for MARSEC Level 1 and MARSEC Level 2, owners or operators of CDC facilities must ensure the facilities are continuously guarded and restricted areas are patrolled.

§ 105.296 Additional requirements—barge fleetings

facilities.

(a) At MARSEC Level 1, in addition to the requirements of this part, an owner or operator of a barge fleeting facility must ensure the implementation of the following security measures:

(1) Designate one or more restricted areas within the barge fleeting facility to handle those barges carrying, in bulk, cargoes regulated by 46 CFR chapter 1, subchapters D or O, or Certain Dangerous Cargoes;

(2) Maintain a current list of vessels and cargoes in the designated restricted area; and

(3) Ensure that at least one towing vessel is available to service the fleeting facility for every 100 barges within the facility.

(b) At MARSEC Level 2, in addition to the requirements of this part and MARSEC Level 1 requirements, an owner or operator of a barge fleeting facility must ensure security personnel are assigned to monitor or patrol the designated restricted area within the barge fleeting facility.

(c) At MARSEC Level 3, in addition to the requirements of this part and MARSEC Level 2 requirements, an owner or operator of a barge fleeting facility must ensure that both land and waterside perimeters of the designated restricted area within the barge fleeting facility are continuously monitored or patrolled.

**Subpart C—Facility Security
Assessment (FSA)**

§ 105.300 General.

(a) The Facility Security Assessment (FSA) is a written document that is based on the collection of background information, the completion of an on-scene survey and an analysis of that information.

(b) A common FSA may be conducted for more than one similar facility provided the FSA reflects any facility-specific characteristics that are unique.

(c) Third parties may be used in any aspect of the FSA if they have the appropriate skills and if the Facility Security Officer (FSO) reviews and accepts their work.

(d) Those involved in a FSA must be able to draw upon expert assistance in the following areas, as appropriate:

(1) Knowledge of current security threats and patterns;

(2) Recognition and detection of dangerous substances and devices;

(3) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

(4) Techniques used to circumvent security measures;

(5) Methods used to cause a security incident;

(6) Effects of dangerous substances and devices on structures and facility services;

(7) Facility security requirements;

(8) Facility and vessel interface business practices;

(9) Contingency planning, emergency preparedness, and response;

(10) Physical security requirements;

(11) Radio and telecommunications systems, including computer systems and networks;

(12) Marine or civil engineering; and

(13) Facility and vessel operations.

**§ 105.305 Facility Security
Assessment (FSA) requirements.**

(a) *Background.* The facility owner or operator must ensure that the following background information, if applicable, is provided to the person or persons who will conduct the assessment:

(1) The general layout of the facility, including:

(i) The location of each active and inactive access point to the facility;

(ii) The number, reliability, and security duties of facility personnel;

(iii) Security doors, barriers, and lighting;

(iv) The location of restricted areas;

(v) The emergency and stand-by equipment available to maintain essential services;

(vi) The maintenance equipment,

cargo spaces, storage areas, and unaccompanied baggage storage;

(vii) Location of escape and evacuation routes and assembly stations; and

(viii) Existing security and safety equipment for protection of personnel and visitors;

(2) Response procedures for fire or other emergency conditions;

(3) Procedures for monitoring facility and vessel personnel, vendors, repair technicians, and dock workers;

(4) Existing contracts with private security companies and existing agreements with local or municipal agencies;

(5) Procedures for controlling keys and other access prevention systems;

(6) Procedures for cargo and vessel stores operations;

(7) Response capability to security incidents;

(8) Threat assessments, including the purpose and methodology of the assessment, for the port in which the facility is located or at which passengers embark or disembark;

(9) Previous reports on security needs; and

(10) Any other existing security procedures and systems, equipment, communications, and facility personnel.

(b) *On-scene survey.* The facility owner or operator must ensure that an on-scene survey of each facility is conducted. The on-scene survey examines and evaluates existing facility protective measures, procedures, and operations to verify or collect the information required in paragraph (a) of this section.

(c) *Analysis and recommendations.* In conducting the FSA, the facility owner or operator must ensure that the FSO analyzes the facility background information and the on-scene survey, and considering the requirements of this part, provides recommendations to establish and prioritize the security measures that should be included in the FSP. The analysis must consider:

(1) Each vulnerability found during the on-scene survey including but not limited to:

(i) Waterside and shore-side

access to the facility and vessel berthing at the facility;

(ii) Structural integrity of the piers, facilities, and associated structures;

(iii) Existing security measures and procedures, including identification systems;

(iv) Existing security measures and procedures relating to services and utilities;

(v) Measures to protect radio and telecommunication equipment, including computer systems and networks;

(vi) Adjacent areas that may be exploited during or for an attack;

(vii) Areas that may, if damaged or used for illicit observation, pose a risk to people, property, or operations within the facility;

(viii) Existing agreements with private security companies providing waterside and shore-side security services;

(ix) Any conflicting policies between safety and security measures and procedures;

(x) Any conflicting facility operations and security duty assignments;

(xi) Any enforcement and personnel constraints;

(xii) Any deficiencies identified during daily operations or training and drills; and

(xiii) Any deficiencies identified following security incidents or alerts, the report of security concerns, the exercise of control measures, or audits;

(2) Possible security threats, including but not limited to:

(i) Damage to or destruction of the facility or of a vessel moored at the facility;

(ii) Hijacking or seizure of a vessel moored at the facility or of persons on board;

(iii) Tampering with cargo, essential equipment or systems, or stores of a vessel moored at the facility;

(iv) Unauthorized access or use including the presence of stowaways;

(v) Smuggling dangerous substances and devices to the facility;

(vi) Use of a vessel moored at the facility to carry those intending to cause a security incident and their equipment;

(vii) Use of a vessel moored at the facility as a weapon or as a means to cause damage or destruction;

(viii) Impact on the facility and its operations due to a blockage of entrances, locks, and approaches; and

(ix) Use of the facility as a transfer point for nuclear, biological, radiological, explosive, or chemical weapons;

(3) Threat assessments by Government agencies;

(4) Vulnerabilities, including human factors, in the facility's infrastructure, policies and procedures;

(5) Any particular aspects of the facility, including the vessels using the facility, which make it likely to be the target of an attack;

(6) Likely consequences in terms of loss of life, damage to property, and economic disruption, including disruption to transportation systems, of an attack on or at the facility; and

(7) Locations where access restrictions or prohibitions will be applied for each MARSEC Level.

(d) *FSA report.* (1) The facility owner or operator must ensure that a written FSA report is prepared and included as part of the FSP. The report must contain:

(i) A summary of how the on-scene survey was conducted;

(ii) A description of existing security measures, including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control, and similar systems;

(iii) A description of each vulnerability found during the on-scene survey;

(iv) A description of security measures that could be used to address each vulnerability;

(v) A list of the key facility operations that are important to protect; and

(vi) A list of identified weaknesses, including human factors, in the infrastructure, policies, and procedures of the facility.

(2) A FSA report must describe the following elements within the facility:

(i) Physical security;

(ii) Structural integrity;

(iii) Personnel protection systems;

(iv) Procedural policies;

(v) Radio and telecommunication systems, including computer systems and networks;

(vi) Relevant transportation infrastructure; and

(vii) Utilities.

(3) The FSA report must list the persons, activities, services, and operations that are important to protect, in each of the following categories:

(i) Facility personnel;

(ii) Passengers, visitors, vendors, repair technicians, vessel personnel, etc.;

(iii) Capacity to maintain emergency response;

(iv) Cargo, particularly dangerous goods and hazardous substances;

(v) Delivery of vessel stores;

(vi) Any facility security communication and surveillance systems; and

(vii) Any other facility security systems, if any.

(4) The FSA report must account for any vulnerabilities in the following areas:

(i) Conflicts between safety and security measures;

(ii) Conflicts between duties and security assignments;

(iii) The impact of watch-keeping duties and risk of fatigue on facility personnel alertness and performance;

(iv) Security training deficiencies; and

(v) Security equipment and systems, including communication systems.

(5) The FSA report must discuss and evaluate key facility measures and operations, including:

(i) Ensuring performance of all security duties;

(ii) Controlling access to the facility, through the use of identification systems or otherwise;

(iii) Controlling the embarkation of vessel personnel and other persons and their effects (including personal effects and baggage whether accompanied or unaccompanied);

(iv) Procedures for the handling of cargo and the delivery of vessel

stores;

(v) Monitoring restricted areas to ensure that only authorized persons have access;

(vi) Monitoring the facility and areas adjacent to the pier; and

(vii) The ready availability of security communications, information, and equipment.

(e) The FSA, FSA report, and FSP must be protected from unauthorized access or disclosure.

§ 105.310 Submission requirements.

(a) A completed FSA report must be submitted with the Facility Security Plan required in § 105.410 of this part.

(b) A facility owner or operator may generate and submit a report that contains the Facility Security Assessment for more than one facility subject to this part, to the extent that they share similarities in design and operations, if authorized and approved by the cognizant COTP.

(c) The FSA must be reviewed and validated, and the FSA report must be updated each time the FSP is submitted for reapproval or revisions.

Subpart D—Facility Security Plan (FSP)

§ 105.400 General.

(a) The Facility Security Officer (FSO) must ensure a Facility Security Plan (FSP) is developed and implemented for each facility for which he or she is designated as FSO. The FSP:

(1) Must identify the FSO by name and position, and provide 24-hour contact information;

(2) Must be written in English;

(3) Must address each vulnerability identified in the Facility Security Assessment (FSA);

(4) Must describe security measures for each MARSEC Level; and

(5) May cover more than one facility to the extent that they share similarities in design and operations, if authorized and approved by the cognizant COTP.

(b) The FSP must be submitted for approval to the cognizant COTP in

a written or electronic format. Information for submitting the FSP electronically can be found at <http://www.uscg.mil/HQ/MSC>.

(c) The FSP is sensitive security information and must be protected in accordance with 49 CFR part 1520.

(d) If the FSP is kept in an electronic format, procedures must be in place to prevent its unauthorized deletion, destruction, or amendment.

§ 105.405 Format and content of the Facility Security Plan (FSP).

(a) A facility owner or operator must ensure that the FSP consists of the individual sections listed in this paragraph (a). If the FSP does not follow the order as it appears in the list, the facility owner or operator must ensure that the FSP contains an index identifying the location of each of the following sections:

(1) Security administration and organization of the facility;

(2) Personnel training;

(3) Drills and exercises;

(4) Records and documentation;

(5) Response to change in MARSEC Level;

(6) Procedures for interfacing with vessels;

(7) Declaration of Security (DoS);

(8) Communications;

(9) Security systems and equipment maintenance;

(10) Security measures for access control, including designated public access areas;

(11) Security measures for restricted areas;

(12) Security measures for handling cargo;

(13) Security measures for delivery of vessel stores and bunkers;

(14) Security measures for monitoring;

(15) Security incident procedures;

(16) Audits and security plan amendments;

(17) Facility Security Assessment (FSA) report; and

(18) Facility Vulnerability and Security Measures Summary (Form CG-6025) in appendix A to part 105—Facility Vulnerability and Security

Measures Summary (CG-6025).

(b) The facility owner or operator must ensure that the FSP describes in detail how each of the individual requirements of subpart B of this part will be met.

(c) The Facility Vulnerability and Security Measures Summary (Form CG-6025) must be completed using information in the FSA concerning identified vulnerabilities and information in the FSP concerning security measures in mitigation of these vulnerabilities.

§ 105.410 Submission and approval.

(a) On or before December 31, 2003, the owner or operator of each facility currently in operation must either:

(1) Submit one copy of their Facility Security Plan (FSP) for review and approval to the cognizant COTP and a letter certifying that the FSP meets applicable requirements of this part; or

(2) If intending to operate under an Approved Security Program, a letter signed by the facility owner or operator stating which approved Alternative Security Program the owner or operator intends to use.

(b) Owners or operators of facilities not in service on or before December 31, 2003, must comply with the requirements in paragraph (a) of this section 60 days prior to beginning operations or by December 31, 2003, whichever is later.

(c) The cognizant COTP will examine each submission for compliance with this part and either:

(1) Approve it and specify any conditions of approval, returning to the submitter a letter stating its acceptance and any conditions;

(2) Return it for revision, returning a copy to the submitter with brief descriptions of the required revisions; or

(3) Disapprove it, returning a copy to the submitter with a brief statement of the reasons for disapproval.

(d) An FSP may be submitted and approved to cover more than one facility where they share similarities in design and operations, if authorized and

approved by each cognizant COTP.

(e) Each facility owner or operator that submits one FSP to cover two or more facilities of similar design and operation must address facility-specific information that includes the design and operational characteristics of each facility and must complete a separate Facility Vulnerability and Security Measures Summary (Form CG-6025), in appendix A to part 105—Facility Vulnerability and Security Measures Summary (CG-6025), for each facility covered by the plan.

(f) A FSP that is approved by the cognizant COTP is valid for five years from the date of its approval.

§ 105.415 Amendment and audit.

(a) *Amendments.* (1) Amendments to a Facility Security Plan (FSP) that is approved by the cognizant COTP may be initiated by:

(i) The facility owner or operator; or

(ii) The cognizant COTP upon a determination that an amendment is needed to maintain the facility's security. The cognizant COTP, who will give the facility owner or operator written notice and request that the facility owner or operator propose amendments addressing any matters specified in the notice. The facility owner or operator will have at least 60 days to submit its proposed amendments. Until amendments are approved, the facility owner or operator shall ensure temporary security measures are implemented to the satisfaction of the COTP.

(2) Proposed amendments must be submitted to the cognizant COTP. If initiated by the facility owner or operator, the proposed amendment must be submitted at least 30 days before the amendment is to take effect unless the cognizant COTP allows a shorter period. The cognizant COTP will approve or disapprove the proposed amendment in accordance with § 105.410 of this subpart.

(3) Nothing in this section should be construed as limiting the facility owner or operator from the timely implementation of such additional security measures not

enumerated in the approved FSP as necessary to address exigent security situations. In such cases, the owner or operator must notify the cognizant COTP by the most rapid means practicable as to the nature of the additional measures, the circumstances that prompted these additional measures, and the period of time these additional measures are expected to be in place.

(4) If there is a change in the owner or operator, the Facility Security Officer (FSO) must amend the FSP to include the name and contact information of the new facility owner or operator and submit the affected portion of the FSP for review and approval in accordance with § 105.410 of this subpart.

(b) *Audits.* (1) The FSO must ensure an audit of the FSP is performed annually, beginning no later than one year from the initial date of approval, and attach a letter to the FSP certifying that the FSP meets the applicable requirements of this part.

(2) The FSP must be audited if there is a change in the facility's ownership or operator, or if there have been modifications to the facility, including but not limited to physical structure, emergency response procedures, security measures, or operations.

(3) Auditing the FSP as a result of modifications to the facility may be limited to those sections of the FSP affected by the facility modifications.

(4) Unless impracticable due to the size and nature of the company or the facility, personnel conducting internal audits of the security measures specified in the FSP or evaluating its implementation must:

(i) Have knowledge of methods for conducting audits and inspections, and security, control, and monitoring techniques;

(ii) Not have regularly assigned security duties; and

(iii) Be independent of any security measures being audited.

(5) If the results of an audit require amendment of either the FSA or FSP, the FSO must submit, in accordance with § 105.410 of this subpart, the amendments to the cognizant COTP for review and approval no later than 30 days after completion of the audit and a letter certifying that the amended FSP meets the applicable requirements of this part.

Facility Vulnerability and Security Measures Summary
Form CG-6025

<small>U.S. DEPARTMENT OF HOMELAND SECURITY U.S. COAST GUARD CG-6025 (05/03)</small>	FACILITY VULNERABILITY AND SECURITY MEASURES SUMMARY	<small>OMB APPROVAL NO. 1625-0077</small>																				
<small>An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a valid OMB control number. The Coast Guard estimates that the average burden for this report is 60 minutes. You may submit any comments concerning the accuracy of this burden estimate or any suggestions for reducing the burden to: Commandant (G-HP), U.S. Coast Guard, 2100 2nd St, SW, Washington D.C. 20593-0001 or Office of Management and Budget, Paperwork Reduction Project (1625-0077), Washington, DC 20503.</small>																						
FACILITY IDENTIFICATION																						
1. Name of Facility																						
2. Address of Facility		3. Latitude																				
		4. Longitude																				
		5. Captain of the Port Zone																				
6. Type of Operation (check all that apply)																						
<table style="width: 100%;"><tr><td><input type="checkbox"/> Break Bulk</td><td><input type="checkbox"/> Petroleum</td><td><input type="checkbox"/> Certain Dangerous Cargo</td><td><input type="checkbox"/> Passengers (Subchapter H)</td><td><input type="checkbox"/> If other, explain below:</td></tr><tr><td><input type="checkbox"/> Dry Bulk</td><td><input type="checkbox"/> Chemical</td><td><input type="checkbox"/> Barge Flooting</td><td><input type="checkbox"/> Passengers (Ferries)</td><td></td></tr><tr><td><input type="checkbox"/> Container</td><td><input type="checkbox"/> LHG/LNG</td><td><input type="checkbox"/> Offshore Support</td><td><input type="checkbox"/> Passengers (Subchapter K)</td><td></td></tr><tr><td><input type="checkbox"/> RO-RO</td><td><input type="checkbox"/> Explosives and other dangerous cargo</td><td><input type="checkbox"/> Military Supply</td><td></td><td></td></tr></table>			<input type="checkbox"/> Break Bulk	<input type="checkbox"/> Petroleum	<input type="checkbox"/> Certain Dangerous Cargo	<input type="checkbox"/> Passengers (Subchapter H)	<input type="checkbox"/> If other, explain below:	<input type="checkbox"/> Dry Bulk	<input type="checkbox"/> Chemical	<input type="checkbox"/> Barge Flooting	<input type="checkbox"/> Passengers (Ferries)		<input type="checkbox"/> Container	<input type="checkbox"/> LHG/LNG	<input type="checkbox"/> Offshore Support	<input type="checkbox"/> Passengers (Subchapter K)		<input type="checkbox"/> RO-RO	<input type="checkbox"/> Explosives and other dangerous cargo	<input type="checkbox"/> Military Supply		
<input type="checkbox"/> Break Bulk	<input type="checkbox"/> Petroleum	<input type="checkbox"/> Certain Dangerous Cargo	<input type="checkbox"/> Passengers (Subchapter H)	<input type="checkbox"/> If other, explain below:																		
<input type="checkbox"/> Dry Bulk	<input type="checkbox"/> Chemical	<input type="checkbox"/> Barge Flooting	<input type="checkbox"/> Passengers (Ferries)																			
<input type="checkbox"/> Container	<input type="checkbox"/> LHG/LNG	<input type="checkbox"/> Offshore Support	<input type="checkbox"/> Passengers (Subchapter K)																			
<input type="checkbox"/> RO-RO	<input type="checkbox"/> Explosives and other dangerous cargo	<input type="checkbox"/> Military Supply																				
VULNERABILITY AND SECURITY MEASURES																						
7a. Vulnerability		7b. Vulnerability Category																				
		<input type="checkbox"/> If other, explain																				
8a. Selected Security Measures (MARSEC Level 1)		8b. Security Measures Category																				
		<input type="checkbox"/> If other, explain																				
9a. Selected Security Measures (MARSEC Level 2)		9b. Security Measures Category																				
		<input type="checkbox"/> If other, explain																				
10a. Selected Security Measures (MARSEC Level 3)		10b. Security Measures Category																				
		<input type="checkbox"/> If other, explain																				
VULNERABILITY AND SECURITY MEASURES																						
7a. Vulnerability		7b. Vulnerability Category																				
		<input type="checkbox"/> If other, explain																				
8a. Selected Security Measures (MARSEC Level 1)		8b. Security Measures Category																				
		<input type="checkbox"/> If other, explain																				
9a. Selected Security Measures (MARSEC Level 2)		9b. Security Measures Category																				
		<input type="checkbox"/> If other, explain																				
10a. Selected Security Measures (MARSEC Level 3)		10b. Security Measures Category																				
		<input type="checkbox"/> If other, explain																				

Vulnerability and Security Measures Addendum Form CG-6025A

U.S. DEPARTMENT OF HOMELAND SECURITY U.S. COAST GUARD CG-6025A (05/03)	VULNERABILITY AND SECURITY MEASURES ADDENDUM	OMB APPROVAL NO. 1625-0077
An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a valid OMB control number. The Coast Guard estimates that the average burden for this report is 60 minutes. You may submit any comments concerning the accuracy of this burden estimate or any suggestions for reducing the burden to: Commandant (CG-MP), U.S. Coast Guard, 2100 2nd St. SW, Washington D.C. 20593-0001 or Office of Management and Budget, Paperwork Reduction Project (1625-0077), Washington, DC 20503. This form may only be used in addition to form CG-6025, never alone.		
NAME OF FACILITY (Use same Name as Block 1., of CG-6025)		
7a. Vulnerability	7b. Vulnerability Category	
	<input type="checkbox"/> If other, explain	
8a. Selected Security Measures (MARSEC Level 1)	8b. Security Measures Category	
	<input type="checkbox"/> If other, explain	
9a. Selected Security Measures (MARSEC Level 2)	9b. Security Measures Category	
	<input type="checkbox"/> If other, explain	
10a. Selected Security Measures (MARSEC Level 3)	10b. Security Measures Category	
	<input type="checkbox"/> If other, explain	
7a. Vulnerability	7b. Vulnerability Category	
	<input type="checkbox"/> If other, explain	
8a. Selected Security Measures (MARSEC Level 1)	8b. Security Measures Category	
	<input type="checkbox"/> If other, explain	
9a. Selected Security Measures (MARSEC Level 2)	9b. Security Measures Category	
	<input type="checkbox"/> If other, explain	
10a. Selected Security Measures (MARSEC Level 3)	10b. Security Measures Category	
	<input type="checkbox"/> If other, explain	
7a. Vulnerability	7b. Vulnerability Category	
	<input type="checkbox"/> If other, explain	
8a. Selected Security Measures (MARSEC Level 1)	8b. Security Measures Category	
	<input type="checkbox"/> If other, explain	
9a. Selected Security Measures (MARSEC Level 2)	9b. Security Measures Category	
	<input type="checkbox"/> If other, explain	
10a. Selected Security Measures (MARSEC Level 3)	10b. Security Measures Category	
	<input type="checkbox"/> If other, explain	

Instructions For the Form CG-6025

INSTRUCTIONS FOR THE CG-6025 FACILITY VULNERABILITY AND SECURITY MEASURES SUMMARY

This form satisfies the requirements for Facility Vulnerability and Security Measures Summary submission found in the Code of Federal Regulations for Facility Security, Form CG-6025A. Vulnerability and Security Measures Addendum, may be used as a continuation of form CG-6025, in order to submit additional vulnerabilities and security measures. If a facility owner or operator submits a Facility Vulnerability and Security Measures Summary pertaining to more than one facility, form CG-6025, shall be submitted to document each additional facility.

BLOCK 1	Self-Explanatory.	BLOCK 8b	Enter the security measures identification code from the KEY to categorically identify the security measure you described. More than one category may be used. If you select other, please explain in the box provided.
BLOCK 2	Street Address.		
BLOCK 3	If available, provide latitude to nearest tenth of a minute.		
BLOCK 4	If available, provide longitude to nearest tenth of a minute.	BLOCK 9a	Enter a concise description of additional selected security measures, if any, that will be applied during MARSEC Level 2 that will mitigate the vulnerability you addressed.
BLOCK 5	Provide the Captain of the Port Zone from the list below in which your facility resides. Their respective zones are described in 33 CFR Part 3.	BLOCK 9b	Enter the security measures identification code from the KEY to categorically identify the security measure you described. More than one category may be used. If you select other, please explain in the box provided.
BLOCK 6	Check all applicable operations that are conducted at your facility. If you select other, please explain in the box provided.		
BLOCK 7a	Enter a concise description of a vulnerability identified in your facility's assessment. Provide location information if appropriate.	BLOCK 10a	Enter a concise description of additional selected security measures, if any, that will be applied during MARSEC Level 3 that will mitigate the vulnerability you addressed.
BLOCK 7b	Enter the vulnerability identification code from the KEY to categorically identify the vulnerability you described. More than one category may be used. If you select other, please explain in the box provided.	BLOCK 10b	Enter the security measures identification code from the KEY to categorically identify the security measure you described. More than one category may be used. If you select other, please explain in the box provided.
BLOCK 8a	Enter a concise description of a selected security measure identified in the plan for MARSEC Level 1 that will mitigate the vulnerability you addressed.		

CAPTAIN OF THE PORT ZONE:

Anchorage	Honolulu	Mobile	Puget Sound
Baltimore	Houston-Galveston	Morgan City	San Diego
Boston	Huntington	New Orleans	San Francisco
Buffalo	Jacksonville	New York	San Juan
Charleston	Juneau	Paducah	Sault Ste. Marie
Chicago	Long Island Sound	Philadelphia	Savannah
Cleveland	Los Angeles/Long Beach	Pittsburgh	St. Louis
Corpus Christi	Louisville	Port Arthur	Tampa
Detroit	Memphis	Portland, ME	Toledo
Duluth	Miami	Portland, OR	Valdez
Guam	Milwaukee	Providence	Wilmington
Hampton Roads			

Key For the Form CG-6025

KEY

VULNERABILITY CATEGORY:

Physical Security	PHS	That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against terrorism, espionage, sabotage, damage, and theft.
Structural Integrity	STI	The design and material construction characteristics of piers, facilities, and associated structures.
Transportation Infrastructure	TRI	Infrastructure that may be exploited during an attack, other than utilities.
Utilities	UTI	The essential equipment and services that are vital to the operation of the facility.
Radio & Telecommunications	RAT	That part of security concerned with measures to protect radio and telecommunication equipment, including computer systems and networks.
Personnel Protection Systems	PPS	Equipment, Gear, or Systems designed to protect facility personnel (i.e. weapons, body armor).
Procedural Policies	PRP	Plans, Policies, and Procedures for specific operations.
Coordination and Information Sharing	CIS	The ability to coordinate and receive/share information with local/state/federal agencies and other commercial entities.
Preparedness	PRE	Implementation of Plans, Policies, and Procedures through Training, Drills, and Exercises conducted to improve security awareness, prevention, and response.

SECURITY MEASURES

Access Control	ACC	Lighting	LIT
Barriers	BAR	Patrols	PAT
Cargo Control	CAC	Planning, Policies, & Procedures	PPP
Communications	COM	Redundancy	RED
Coordination	COR	Response	RES
Credentialing	CRE	Stand-off Distance	SOD
Detection	DET	Structural Hardening	STH
Guard Force	GUF	Surveillance	SUR
IT Security	ITS	Training	TRA
Inspections	INS	Vessels/Vehicles	VEV
Intelligence	INT		

33 CFR
Navigation and Navigable Waters
CHAPTER I
COAST GUARD, DEPARTMENT
OF HOMELAND SECURITY
SUBCHAPTER H -- MARITIME
SECURITY

PART 106—MARITIME
SECURITY: OUTER
CONTINENTAL SHELF (OCS)
FACILITIES

Subpart A -- General

Sec.

- 106.100 Definitions.
- 106.105 Applicability.
- 106.110 Compliance dates.
- 106.115 Compliance documentation.
- 106.120 Noncompliance.
- 106.125 Waivers.
- 106.130 Equivalents.
- 106.135 Alternative Security Program.
- 106.140 Maritime Security (MARSEC) Directive.
- 106.145 Right to appeal.

Subpart B -- Outer Continental Shelf (OCS) Facility Security Requirements

- 106.200 Owner or operator.
- 106.205 Company Security Officer (CSO).
- 106.210 Facility Security Officer (FSO).
- 106.215 Company or OCS facility personnel with security duties.
- 106.220 Security training for all other OCS facility personnel.
- 106.225 Drill and exercise requirements.
- 106.230 OCS facility recordkeeping requirements.
- 106.235 Maritime Security (MARSEC) Level coordination and implementation.
- 106.240 Communications.
- 106.245 Procedures for interfacing with vessels.
- 106.250 Declaration of Security (DoS).
- 106.255 Security systems and equipment maintenance.

- 106.260 Security measures for access control.
- 106.265 Security measures for restricted areas.
- 106.270 Security measures for delivery of stores and industrial supplies.
- 106.275 Security measures for monitoring.
- 106.280 Security incident procedures.

Subpart C -- Outer Continental Shelf (OCS) Facility Security Assessment (FSA)

- 106.300 General.
- 106.305 Facility Security Assessment (FSA) requirements.
- 106.310 Submission requirements.

Subpart D -- Outer Continental Shelf (OCS) Facility Security Plan (FSP)

- 106.400 General.
- 106.405 Format and Content of the Facility Security Plan (FSP).
- 106.410 Submission and approval.
- 106.415 Amendment and audit.

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. Chapter 701; 50 U.S.C. 191; 33 CFR 1.05–1, 6.04–11, 6.14, 6.16, and 6.19; Department Of Homeland Security Delegation No. 0170.1.

Source: USCG-2003-14759, 68 FR 39322, July 1, 2003, unless otherwise noted.

Subpart A—General

§ 106.100 Definitions.

Except as specifically stated in this subpart, the definitions in part 101 of this subchapter apply to this part.

§ 106.105 Applicability.

The requirements in this part apply to owners and operators of any fixed or floating facility, including MODUs not subject to part 104 of this subchapter, operating on the Outer Continental Shelf (OCS) of the United States for the purposes of engaging in the exploration, development, or production of oil, natural gas, or mineral resources that are regulated by 33 CFR subchapter N, that meet the following operating

conditions:

- (a) Hosts more than 150 persons for 12 hours or more in each 24-hour period continuously for 30 days or more;
- (b) Produces greater than 100,000 barrels of oil per day; or
- (c) Produces greater than 200 million cubic feet of natural gas per day.

§ 106.110 Compliance dates.

(a) On or before December 31, 2003, OCS facility owners or operators must submit to the cognizant District Commander for each OCS facility—

(1) The Facility Security Plan described in subpart D of this part for review and approval; or

(2) If intending to operate under an approved Alternative Security Program, a letter signed by the OCS facility owner or operator stating which approved Alternative Security Program the owner or operator intends to use.

(b) On or before July 1, 2004, each OCS facility owner or operator must be operating in compliance with this part.

(c) OCS facilities built on or after July 1, 2004, must submit for approval an FSP 60 days prior to beginning operations.

§ 106.115 Compliance documentation.

Each OCS facility owner or operator subject to this part must ensure before July 1, 2004, that copies of the following documentation are available at the OCS facility and are made available to the Coast Guard upon request:

(a) The approved Facility Security Plan (FSP) and any approved revisions or amendments thereto, and a letter of approval from the cognizant District Commander dated within the last 5 years;

(b) The FSP submitted for approval and current written acknowledgment from the cognizant District Commander, stating that the Coast Guard is currently reviewing the FSP submitted for approval and that the OCS facility may continue to operate so long as the OCS facility remains in compliance with the submitted FSP; or

(c) For OCS facilities operating under a Coast Guard-approved Alternative Security Program as provided in §106.135, a copy of the Alternative Security Program the OCS facility is using, including a facility specific security assessment report generated under the Alternative Security Program, as specified in § 101.120(b)(3) of this subchapter, and a letter signed by the OCS facility owner or operator, stating which Alternative Security Program the OCS facility is using and certifying that the OCS facility is in full compliance with that program.

§ 106.120 Noncompliance.

When an OCS facility must temporarily deviate from the requirements of this part, the OCS facility owner or operator must notify the cognizant District Commander, and either suspend operations or request and receive permission from the District Commander to continue operating.

§ 106.125 Waivers.

Any OCS facility owner or operator may apply for a waiver of any requirement of this part that the OCS facility owner or operator considers unnecessary in light of the nature or operating conditions of the OCS facility. A request for a waiver must be submitted in writing with justification to the cognizant District Commander. The cognizant District Commander may require the OCS facility owner or operator to provide additional data for use in determining the validity of the requested waiver. The cognizant District Commander may grant a waiver, in writing, with or without conditions only if the waiver will not reduce the overall security of the OCS facility, its personnel, or visiting vessels.

§ 106.130 Equivalents.

For any measure required by this part, the OCS facility owner or operator may propose an equivalent, as provided in §101.130 of this subchapter.

§ 106.135 Alternative Security Program.

An OCS facility owner or operator may use an Alternative Security Program approved under §101.120 of this subchapter if:

(a) The Alternative Security Program is appropriate to that OCS facility;

(b) The OCS facility does not serve vessels on international voyages; and

(c) The Alternative Security Program is implemented in its entirety.

§ 106.140 Maritime Security (MARSEC) Directive.

All OCS facility owners or operators subject to this part must comply with any instructions contained in a MARSEC Directive issued under §101.405 of this subchapter.

§ 106.145 Right to appeal.

Any person directly affected by a decision or action taken under this part, by or on behalf of the Coast Guard, may appeal as described in §101.420 of this subchapter.

Subpart B—Outer Continental Shelf (OCS) Facility Security Requirements

§ 106.200 Owner or operator.

(a) Each OCS facility owner or operator must ensure that the OCS facility operates in compliance with the requirements of this part.

(b) For each OCS facility, the OCS facility owner or operator must:

(1) Define the security organizational structure for each OCS Facility and provide each person exercising security duties or responsibilities within that structure the support needed to fulfill those obligations;

(2) Designate in writing, by name or title, a Company Security Officer (CSO) and a Facility Security Officer (FSO) for each OCS Facility and identify how those officers can be contacted at any time;

(3) Ensure that a Facility Security Assessment (FSA) is conducted;

(4) Ensure the development and submission for approval of a Facility

Security Plan (FSP);

(5) Ensure that the OCS facility operates in compliance with the approved FSP;

(6) Ensure that adequate coordination of security issues takes place between OCS facilities and vessels, including the execution of a Declaration of Security (DoS) as required by this part;

(7) Ensure, within 12 hours of notification of an increase in MARSEC Level, implementation of the additional security measures required by the FSP for the new MARSEC Level;

(8) Ensure all breaches of security and security incidents are reported in accordance with part 101 of this subchapter; and

(9) Ensure consistency between security requirements and safety requirements.

§ 106.205 Company Security Officer (CSO).

(a) *General.* (1) An OCS facility owner or operator may designate a single CSO for all its OCS facilities to which this part applies, or may designate more than one CSO, in which case the owner or operator must clearly identify the OCS facilities for which each CSO is responsible.

(2) A CSO may perform other duties within the owner's or operator's organization, including the duties of a Facility Security Officer, provided he or she is able to perform the duties and responsibilities required of the CSO.

(3) The CSO may delegate duties required by this part, but remains responsible for the performance of those duties.

(b) *Qualifications.* The CSO must have general knowledge, through training or equivalent job experience, in the following:

(1) Security administration and organization of the OCS facility;

(2) OCS facility and vessel operations and conditions;

(3) OCS facility and vessel security measures including the meaning and consequential requirements of the different MARSEC Levels;

(4) Emergency preparedness and

response and contingency planning;

(5) Security equipment and systems and their operational limitations;

(6) Methods of conducting audits, inspection, control, and monitoring; and

(7) Techniques for security training and education, including security measures and procedures.

(c) In addition to the knowledge and training in paragraph (b) of this section, the CSO must have general knowledge, through training or equivalent job experience, in the following, as appropriate:

(1) Relevant international conventions, codes, and recommendations;

(2) Relevant government legislation and regulations;

(3) Responsibilities and functions of other security organizations;

(4) Methodology of Facility Security Assessment.

(5) Methods of OCS facility security surveys and inspections;

(6) Handling sensitive security information (SSI) and security related communications;

(7) Knowledge of current security threats and patterns;

(8) Recognition and detection of dangerous substances and devices;

(9) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

(10) Techniques used to circumvent security measures;

(11) Methods of physical screening and non-intrusive inspections; and

(12) Conducting and assessing security drills and exercises.

(d) *Responsibilities.* In addition to any other duties required by this part, for each OCS facility for which the CSO is responsible, the CSO must:

(1) Keep the OCS facility apprised of potential threats or other information relevant to its security;

(2) Ensure that a Facility Security Assessment (FSA) is carried out in compliance with this part;

(3) Ensure that a Facility Security Plan (FSP) is developed,

approved, maintained, and implemented in compliance with this part;

(4) Ensure that the FSP is modified when necessary to comply with this part;

(5) Ensure that OCS facility security activities are audited in compliance with this part;

(6) Ensure the timely correction of problems identified by audits or inspections;

(7) Enhance security awareness and vigilance within the owner's or operator's organization;

(8) Ensure relevant personnel receive adequate security training in compliance with this part;

(9) Ensure communication and cooperation between the OCS facility and vessels that interface with it, in compliance with this part;

(10) Ensure consistency between security requirements and safety requirements in compliance with this part;

(11) Ensure that if a common FSP is prepared for more than one similar OCS facility, the FSP reflects any OCS facility specific characteristics; and

(12) Ensure compliance with an Alternative Security Program or equivalents approved under this subchapter, if appropriate.

§ 106.210 OCS Facility Security Officer (FSO).

(a) *General.* (1) The FSO may perform other duties within the owner's or operator's organization, provided he or she is able to perform the duties and responsibilities required of the FSO of each such OCS facility.

(2) The same person may serve as the FSO for more than one OCS facility, provided the facilities are within a reasonable proximity to each other. If a person serves as the FSO for more than one OCS facility, the name of each OCS facility for which he or she is the FSO must be listed in the Facility Security Plan (FSP) of each OCS facility for which he or she is the FSO.

(3) The FSO may assign security duties to other OCS facility personnel; however, the FSO remains responsible for these duties.

(b) *Qualifications.* The FSO must have general knowledge, through training or equivalent job experience, in the following:

(1) Those items listed in §106.205(b), and as appropriate §106.205(c), of this part;

(2) OCS facility layout;

(3) The FSP and related procedures; and

(4) Operation, testing and maintenance of security equipment and systems.

(c) *Responsibilities.* In addition to any other responsibilities specified elsewhere in this part, the FSO must, for each OCS facility for which he or she has been designated:

(1) Regularly inspect the OCS facility to ensure that security measures are maintained in compliance with this part;

(2) Ensure the maintenance of and supervision of the implementation of the FSP, and any amendments to the FSP, in compliance with this part;

(3) Ensure the coordination and handling of stores and industrial supplies in compliance with this part;

(4) Where applicable, propose modifications to the FSP to the Company Security Officer (CSO);

(5) Ensure that any problems identified during audits or inspections are reported to the CSO, and promptly implement any corrective actions;

(6) Ensure security awareness and vigilance on board the OCS facility;

(7) Ensure adequate security training for OCS facility personnel in compliance with this part;

(8) Ensure the reporting and recording of all security incidents in compliance with this part;

(9) Ensure the coordinated implementation of the FSP with the CSO;

(10) Ensure that security equipment is properly operated, tested, calibrated and maintained in compliance with this part;

(11) Ensure consistency between security requirements and the proper treatment of OCS facility personnel affected by those requirements;

(12) Ensure that occurrences that threaten the security of the OCS facility are recorded and reported to the CSO;

(13) Ensure that when changes in the MARSEC Level are attained they are recorded and reported to the CSO, OCS facility owner or operator, and the cognizant District Commander; and

(14) Have prompt access to a copy of the FSA, along with an approved copy of the FSP.

§ 106.215 Company or OCS facility personnel with security duties.

Company or OCS facility personnel responsible for security duties must have knowledge, through training or equivalent job experience, in the following, as appropriate:

(a) Knowledge of current and anticipated security threats and patterns.

(b) Recognition and detection of dangerous substances and devices;

(c) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

(d) Recognition of techniques used to circumvent security measures;

(e) Security related communications;

(f) Knowledge of emergency procedures and contingency plans;

(g) Operation of security equipment and systems;

(h) Testing, calibration, and maintenance of security equipment and systems;

(i) Inspection, control, and monitoring techniques;

(j) Methods of physical screenings of persons, personal effects, stores and industrial supplies;

(k) Relevant provisions of the Facility Security Plan (FSP); and

(l) The meaning and the consequential requirements of the different MARSEC Levels.

§ 106.220 Security training for all other OCS facility personnel.

All other OCS facility personnel, including contractors, whether part-time, full-time, temporary, or permanent, must have knowledge, through training or equivalent job experience, of the following, as appropriate:

(a) Relevant provisions of the

Facility Security Plan (FSP);

(b) The meaning and the consequential requirements of the different MARSEC Levels including emergency procedures and contingency plans;

(c) Recognition and detection of dangerous substances and devices;

(d) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security; and

(e) Recognition of techniques used to circumvent security measures.

§ 106.225 Drill and exercise requirements.

(a) *General.* (1) Drills and exercises must test the proficiency of facility personnel in assigned security duties at all MARSEC Levels and the effective implementation of the Facility Security Plan (FSP). They must enable the Facility Security Officer (FSO) to identify any related security deficiencies that need to be addressed.

(2) A drill or exercise required by this section may be satisfied with the implementation of security measures required by the FSP as the result of an increase in the MARSEC Level, provided the FSO reports attainment to the cognizant District Commander.

(b) *Drills.* (1) From the date of the FSP approval, the FSO must ensure that at least one security drill is conducted every 3 months. Security drills may be held in conjunction with non-security drills, where appropriate.

(2) Drills must test individual elements of the FSP, including response to security threats and incidents. Drills should take into account the types of operations of the OCS facility, OCS facility personnel changes, the types of vessels calling at the OCS facility, and other relevant circumstances. Examples of drills include unauthorized entry to a restricted area, response to alarms, and notification of appropriate authorities.

(3) If a vessel is conducting operations with the OCS facility on the date the OCS facility has planned to conduct any drills, the OCS facility may include, but cannot require, the vessel or vessel personnel to participate in the OCS facility's scheduled drill.

(c) *Exercises.* (1) From the date of the FSP approval, exercises must be conducted at least once each calendar year, with no more than 18 months between exercises.

(2) Exercises may be:

(i) Full scale or live;

(ii) Tabletop simulation;

(iii) Combined with other appropriate exercises held; or

(iv) A combination of the elements in paragraphs (c)(2)(i) through (iii) of this section.

(3) Exercises may be facility-specific or part of a cooperative exercise program.

(4) Each exercise must test communication and notification procedures, and elements of coordination, resource availability, and response.

(5) Exercises are a full test of the Facility Security Plan and must include substantial and active participation of relevant company and OCS facility personnel, and may include governmental authorities and vessels depending on the scope and the nature of the exercise.

§ 106.230 OCS facility recordkeeping requirements.

(a) Unless otherwise specified in this section, the Facility Security Officer (FSO) must keep records of the activities as set out in paragraph (b) of this section for at least 2 years and make them available to the Coast Guard upon request.

(b) Records required by this section may be kept in electronic format. If kept in an electronic format, they must be protected against unauthorized access, deletion, destruction, amendment, and disclosure. The following records must be kept:

(1) *Training.* For training under § 106.215, the date of each session, duration of session, a description of the training, and a list of attendees;

(2) *Drills and exercises.* For each drill or exercise, the date held, a description of the drill or exercise, a list of participants, and any best practices or lessons learned which may improve the FSP;

(3) *Incidents and breaches of security.* Date and time of occurrence, location within the OCS facility, a description of the incident or breach, the identity of the individual to whom it was reported, and a description of the response;

(4) *Changes in MARSEC Levels.* Date and time of the notification received, and the time of compliance with additional requirements;

(5) *Maintenance, calibration, and testing of security equipment.* For each occurrence of maintenance, calibration, and testing, record the date and time, and the specific security equipment involved;

(6) *Security threats.* Date and time of occurrence, how the threat was communicated, who received or identified the threat, a description of the threat, to whom it was reported, and a description of the response;

(7) *Declaration of Security (DoS).* A copy of each DoS for at least 90 days after the end of its effective period; and

(8) *Annual audit of the Facility Security Plan (FSP).* For each annual audit, a letter certified by the FSO stating the date the audit was conducted.

§ 106.235 Maritime Security (MARSEC) Level coordination and implementation.

(a) The OCS facility owner or operator must ensure the OCS facility operates in compliance with the security requirements in this part for the MARSEC Level in effect for the OCS facility.

(b) When notified of an increase in the MARSEC Level, the OCS facility owner or operator must ensure:

(1) Vessels conducting operations with the OCS facility and vessels scheduled to arrive at the OCS facility within 96 hours of the MARSEC Level change are notified of the new MARSEC Level and the Declaration of Security (DoS), if applicable, is revised as necessary;

(2) The OCS facility complies with the required additional security measures within 12 hours; and

(3) The OCS facility reports compliance or noncompliance to the

cognizant District Commander.

(c) For MARSEC Levels 2 and 3, the Facility Security Officer (FSO) must inform all OCS facility personnel about identified threats, emphasize reporting procedures, and stress the need for increased vigilance.

(d) An OCS facility owner or operator whose facility is not in compliance with the requirements of this section must so inform the cognizant District Commander and obtain approval prior to interfacing with another vessel or prior to continuing operations.

§ 106.240 Communications.

(a) The Facility Security Officer (FSO) must have a means to effectively notify OCS facility personnel of changes in security conditions at the OCS facility.

(b) Communication systems and procedures must allow effective and continuous communications between the OCS facility security personnel, vessels interfacing with the OCS facility, the cognizant District Commander, and national and local authorities with security responsibilities.

(c) Facility communications systems must have a backup means for both internal and external communications.

§ 106.245 Procedures for interfacing with vessels.

The OCS facility owner or operator must ensure that there are measures for interfacing with vessels at all MARSEC Levels.

§ 106.250 Declaration of Security (DoS).

(a) Each OCS facility owner or operator must ensure procedures are established for requesting a DoS and for handling DoS requests from vessels.

(b) At MARSEC Level 1, owners or operators of OCS facilities interfacing with a manned vessel carrying Certain Dangerous Cargoes, in bulk, must:

(1) Prior to the arrival of a vessel to the OCS facility, ensure the Facility Security Officer (FSO) and Master,

Vessel Security Officer (VSO), or their designated representatives coordinate security needs and procedures, and agree upon the contents of a DoS for the period of time the vessel is at the OCS facility; and

(2) Upon the arrival of the vessel at the OCS facility, the FSO and Master, VSO, or their designated representatives, must sign the written DoS.

(c) Neither the OCS facility nor the vessel may embark or disembark personnel, or transfer stores or industrial supplies until the DoS has been signed.

(d) At MARSEC Levels 2 and 3, the FSOs of OCS facilities interfacing with manned vessels subject to part 104 of this chapter, or their designated representatives, must sign and implement DoSs as required in paragraphs (b)(1) and (b)(2) of this section.

(e) At MARSEC Levels 1 and 2, FSOs of OCS facilities that frequently interface with the same vessel may implement a continuing DoS for multiple visits, provided that:

(1) The DoS is valid for a specific MARSEC Level;

(2) The effective period at MARSEC Level 1 does not exceed 90 days; and

(3) The effective period at MARSEC Level 2 does not exceed 30 days.

(f) When the MARSEC Level increases beyond that contained in the DoS, the continuing DoS is void and a new DoS must be executed in accordance with this section.

§ 106.255 Security systems and equipment maintenance.

(a) Security systems and equipment must be in good working order and inspected, tested, calibrated, and maintained according to manufacturers' recommendations.

(b) Security systems must be regularly tested in accordance with the manufacturers' recommendations; noted deficiencies corrected promptly; and the results recorded as required in §106.230(b)(5) of this part.

(c) The Facility Security Plan

(FSP) must include procedures for identifying and responding to security system and equipment failures or malfunctions.

§ 106.260 Security measures for access control.

(a) *General.* The OCS facility owner or operator must ensure the implementation of security measures to:

(1) Deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, or the OCS facility;

(2) Secure dangerous substances and devices that are authorized by the OCS facility owner or operator to be on board; and

(3) Control access to the OCS facility.

(b) The OCS facility owner or operator must ensure that the following are specified:

(1) All locations providing means of access to the OCS facility where access restrictions or prohibitions are applied for each security level to prevent unauthorized access;

(2) The identification of the types of restriction or prohibition to be applied and the means of enforcing them; and

(3) The means of identification required to allow individuals to access the OCS facility and remain on the OCS facility without challenge.

(c) The OCS facility owner or operator must ensure that an identification system is established for checking the identification of OCS facility personnel or other persons seeking access to the OCS facility that:

(1) Provides for identification of authorized and unauthorized persons at any MARSEC Level;

(2) Is coordinated, when practicable, with identification systems used by vessels or other transportation conveyances conducting operations with the OCS facility;

(3) Is updated regularly; and

(4) Allows temporary or continuing access for OCS facility personnel and visitors through the use of a badge or other system to verify their identity.

(d) The OCS facility owner or operator must establish in the approved Facility Security Plan (FSP) the frequency of application of any access controls, particularly if they are to be applied on a random or occasional basis.

(e) *MARSEC Level 1.* The OCS facility owner or operator must ensure the following security measures are implemented at the facility:

(1) Screen persons and personal effects going aboard the OCS facility for dangerous substances and devices at the rate specified in the approved FSP;

(2) Conspicuously post signs that describe security measures currently in effect and clearly stating that:

(i) Boarding an OCS facility is deemed valid consent to screening or inspection; and

(ii) Failure to consent or submit to screening or inspection will result in denial or revocation of authorization to be on board;

(3) Check the identification of any person seeking to board the OCS facility, including OCS facility employees, passengers and crews of vessels interfacing with the OCS facility, vendors, and visitors;

(4) Deny or revoke a person's authorization to be on board if the person is unable or unwilling, upon the request of OCS facility personnel, to establish his or her identity or to account for his or her presence on board. Any such incident must be reported in compliance with this part;

(5) Deter unauthorized access to the OCS facility;

(6) Identify access points that must be secured or attended to deter unauthorized access;

(7) Lock or otherwise prevent access to unattended spaces that adjoin areas to which OCS facility personnel and visitors have access;

(8) Ensure OCS facility personnel are not required to engage in or be subjected to screening, of the person or of personal effects, by other OCS facility personnel, unless security clearly requires it;

(9) Provide a designated secure area on board, or in liaison with a vessel

interfacing with the OCS facility, for conducting inspections and screening of people and their personal effects; and

(10) Respond to the presence of unauthorized persons on board.

(f) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the OCS facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved FSP. These additional security measures may include:

(1) Increasing the frequency and detail of screening of people and personal effects embarking onto the OCS facility as specified for MARSEC Level 2 in the approved FSP;

(2) Assigning additional personnel to patrol deck areas during periods of reduced OCS facility operations to deter unauthorized access;

(3) Limiting the number of access points to the OCS facility by closing and securing some access points; or

(4) Deterring waterside access to the OCS facility, which may include, providing boat patrols.

(g) *MARSEC Level 3.* In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, the OCS facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved FSP. The additional security measures may include:

(1) Screening all persons and personal effects for dangerous substances and devices;

(2) Being prepared to cooperate with responders;

(3) Limiting access to the OCS facility to a single, controlled access point;

(4) Granting access to only those responding to the security incident or threat thereof;

(5) Suspending embarkation and/or disembarkation of personnel;

(6) Suspending the onloading of stores or industrial supplies;

(7) Evacuating the OCS facility;

or

(8) Preparing for a full or partial

search of the OCS facility.

§ 106.265 Security measures for restricted areas.

(a) *General.* The OCS facility owner or operator must ensure the designation of restricted areas in order to:

- (1) Prevent or deter unauthorized access;
- (2) Protect persons authorized to be in the OCS facility;
- (3) Protect the OCS facility;
- (4) Protect vessels using and serving the OCS facility;
- (5) Protect sensitive security areas within the OCS facility;
- (6) Protect security and surveillance equipment and systems; and
- (7) Protect stores and industrial supplies from tampering.

(b) *Designation of restricted areas.* The OCS facility owner or operator must ensure restricted areas are designated within the OCS facility. They must also ensure that all restricted areas are clearly marked and indicate that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security. The OCS facility owner or operator may designate the entire OCS facility as a restricted area. Restricted areas must include, as appropriate:

- (1) Areas containing sensitive security information;
- (2) Areas containing security and surveillance equipment and systems and their controls, and lighting system controls; and
- (3) Areas containing critical OCS facility infrastructure equipment, including:
 - (i) Water supplies;
 - (ii) Telecommunications;
 - (iii) Power distribution system;
 - (iv) Access points for ventilation and air-conditioning systems;
 - (v) Manufacturing areas and control rooms;
 - (vi) Areas designated for loading, unloading or storage of stores and industrial supplies; and
 - (vii) Areas containing hazardous materials.

(c) The OCS facility owner or

operator must ensure that the Facility Security Plan (FSP) includes measures for restricted areas to:

- (1) Identify which OCS facility personnel are authorized to have access;
- (2) Determine which persons other than OCS facility personnel are authorized to have access;
- (3) Determine the conditions under which that access may take place;
- (4) Define the extent of any restricted area; and
- (5) Define the times when access restrictions apply.

(d) *MARSEC Level 1.* At MARSEC Level 1, the OCS facility owner or operator must ensure the implementation of security measures to prevent unauthorized access or activities within the area. These security measures may include:

- (1) Restricting access to only authorized personnel;
- (2) Securing all access points not actively used and providing physical barriers to impede movement through the remaining access points;
- (3) Verifying the identification and authorization of all persons seeking entry;
- (4) Using security personnel, automatic intrusion detection devices, surveillance equipment, or surveillance systems to detect unauthorized entry to or movement within restricted areas; or
- (5) Designating temporary restricted areas to accommodate OCS facility operations. If temporary restricted areas are designated, the FSP must include security requirements to conduct a security sweep of the designated temporary restricted areas both before and after the area has been established.

(e) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the OCS facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in their approved FSP. These additional security measures may include:

- (1) Enhancing the effectiveness of the barriers surrounding restricted areas, for example, by the use of patrols or automatic intrusion detection

devices;

(2) Reducing the number of access points to restricted areas, and enhancing the controls applied at the remaining accesses;

(3) Further restricting access to the restricted areas and movements and storage within them;

(4) Using continuously monitored and recorded surveillance equipment;

(5) Increasing the number and frequency of patrols, including the use of waterborne patrols; or

(6) Restricting access to areas adjacent to the restricted areas.

(f) *MARSEC Level 3.* In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the OCS facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in their approved FSP. These additional security measures may include:

(1) Restricting access to additional areas;

(2) Prohibiting access to restricted areas; or

(3) Searching restricted areas as part of a security sweep of all or part of the OCS facility.

§ 106.270 Security measures for delivery of stores and industrial supplies.

(a) *General.* The OCS facility owner or operator must ensure that security measures relating to the delivery of stores or industrial supplies to the OCS facility are implemented to:

(1) Check stores or industrial supplies for package integrity;

(2) Prevent stores or industrial supplies from being accepted without inspection;

(3) Deter tampering; and

(4) Prevent stores and industrial supplies from being accepted unless ordered. For any vessels that routinely use an OCS facility, an OCS facility owner or operator may establish and implement standing arrangements between the OCS facility, its suppliers, and any vessel delivering stores or industrial supplies regarding

notification and the timing of deliveries and their documentation.

(b) *MARSEC Level 1.* At MARSEC Level 1, the OCS facility owner or operator must ensure the implementation of measures to:

(1) Inspect stores or industrial supplies before being accepted; and

(2) Check that stores or industrial supplies match the order prior to being brought on board.

(c) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the OCS facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved Facility Security Plan (FSP). These additional security measures may include:

(1) Intensifying inspection of the stores or industrial supplies during delivery; or

(2) Checking stores or industrial supplies prior to receiving them on board.

(d) *MARSEC Level 3.* In addition to the security measures for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the OCS facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved FSP. These additional security measures may include:

(1) Checking all OCS facility stores or industrial supplies more extensively;

(2) Restricting or suspending delivery of stores or industrial supplies; or

(3) Refusing to accept stores or industrial supplies on board.

§ 106.275 Security measures for monitoring.

(a) *General.* (1) The OCS facility owner or operator must ensure the implementation of security measures in this section and have the capability to continuously monitor, through a combination of lighting, watchkeepers, security guards, deck watches, waterborne patrols, automatic intrusion-detection devices, or

surveillance equipment as specified in their approved Facility Security Plan (FSP), the:

- (i) OCS facility;
- (ii) Restricted areas on board the OCS facility; and
- (iii) The area surrounding the OCS facility.

(2) The following must be considered when establishing the appropriate level and location of lighting:

- (i) OCS facility personnel should be able to detect activities on and around OCS facilities;

(ii) Coverage should facilitate personnel identification at access points; and

- (iii) Lighting effects, such as glare, and their impact on safety, navigation, and other security activities.

(b) *MARSEC Level 1.* At MARSEC Level 1, the OCS facility owner or operator must ensure the implementation of security measures, which may be implemented in coordination with a vessel interfacing with the OCS facility, to:

(1) Monitor the OCS facility, particularly OCS facility access points and restricted areas;

(2) Be able to conduct emergency searches of the OCS facility;

(3) Ensure that equipment or system failures or malfunctions are identified and corrected;

(4) Ensure that any automatic intrusion detection device, sets off an audible or visual alarm, or both, at a location that is continuously attended or monitored; and

(5) Light deck and OCS facility access points during the period between sunset and sunrise and periods of limited visibility sufficiently to allow visual identification of persons seeking access to the OCS facility.

(c) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the OCS facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved FSP. These additional security measures may include:

- (1) Increasing the frequency and

detail of security patrols;

(2) Using (if not already in use) or increasing the use of security and surveillance equipment;

(3) Assigning additional personnel as security lookouts; or

(4) Coordinating with boat patrols, when provided.

(d) *MARSEC Level 3.* In addition to the security measures for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the OCS facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved FSP. These additional security measures may include:

(1) Cooperating with responders;

(2) Switching on all lights;

(3) Switching on all surveillance equipment capable of recording activities on, or in the vicinity of, the OCS facility;

(4) Maximizing the length of time such surveillance equipment (if not already in use) can continue to record; or

(5) Preparing for underwater inspection of the OCS facility.

§ 106.280 Security incident procedures.

For each MARSEC Level, the OCS facility owner or operator must ensure the Facility Security Officer (FSO) and OCS facility security personnel are able to:

(a) Respond to security threats or breaches of security and maintain critical OCS facility and OCS facility-to-vessel interface operations;

(b) Deny access to the OCS facility, except to those responding to an emergency;

(c) Evacuate the OCS facility in case of security threats or breaches of security; and

(d) Report security incidents as required in § 101.305 of this subchapter;

(e) Brief all OCS facility personnel on possible threats and the need for vigilance, soliciting their assistance in reporting suspicious persons, objects, or activities; and

(f) Secure non-critical

operations in order to focus response on critical operations.

Subpart C—Outer Continental Shelf (OCS) Facility Security Assessment (FSA)

§ 106.300 General.

(a) The Facility Security Assessment (FSA) is a written document that is based on the collection of background information, the completion of an on-scene survey and an analysis of that information.

(b) A single FSA may be performed and applied to more than one OCS facility to the extent they share physical characteristics, location, and operations.

(c) Third parties may be used in any aspect of the FSA if they have the appropriate skills and if the Company Security Officer (CSO) reviews and accepts their work.

(d) Those involved in a FSA must be able to draw upon expert assistance in the following areas, as appropriate:

- (1) Knowledge of current and anticipated security threats and patterns;
- (2) Recognition and detection of dangerous substances and devices;
- (3) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;
- (4) Recognition of techniques used to circumvent security measures;
- (5) Methods used to cause a security incident;
- (6) Effects of dangerous substances and devices on structures and essential services;
- (7) OCS facility security requirements;
- (8) OCS facility and vessel interface business practices;
- (9) Contingency planning, emergency preparedness and response;
- (10) Physical security requirements;
- (11) Radio and telecommunications systems, including computer systems and networks;
- (12) Marine or civil engineering;

and

(13) OCS facility and vessel operations.

§ 106.305 Facility Security Assessment (FSA) requirements.

(a) *Background.* The OCS facility owner or operator must ensure that the following background information, if applicable, is provided to the person or persons who will conduct the assessment:

(1) The general layout of the OCS facility, including:

(i) The location of each access point to the OCS facility;

(ii) The number, reliability, and security duties of OCS facility personnel;

(iii) Security doors, barriers, and lighting;

(iv) The location of restricted areas;

(v) The emergency and stand-by equipment available to maintain essential services;

(vi) The essential maintenance equipment and storage areas;

(vii) Location of escape and evacuation routes and assembly stations; and

(viii) Existing security and safety equipment for protection of personnel;

(2) Response procedures for fire or other emergency conditions;

(3) Procedures for monitoring OCS facility and vessel personnel;

(4) Procedures for controlling keys and other access prevention systems;

(5) Response capability for security incidents;

(6) Threat assessments, including the purpose and methodology of the assessment, for the OCS facility's location;

(7) Previous reports on security needs; and

(8) Any other existing security procedures and systems, equipment, communications, and OCS facility personnel.

(b) *On-scene survey.* The OCS facility owner or operator must ensure that an on-scene survey of each OCS facility is conducted. The on-scene survey examines and evaluates existing

OCS facility protective measures, procedures, and operations to verify or collect the information required in paragraph (a) of this section.

(c) *Analysis and recommendations.* In conducting the FSA, the OCS owner or operator must ensure that the Company Security Officer (CSO) analyzes the OCS facility background information and the on-scene survey, and considering the requirements of this part, provides recommendations to establish and prioritize the security measures that should be included in the FSP. The analysis must consider:

(1) Each vulnerability found during the on-scene survey, including but not limited to:

(i) Access to the OCS facility;
(ii) Structural integrity of the OCS facility;

(iii) Existing security measures and procedures, including identification systems;

(iv) Existing security measures and procedures relating to essential services;

(v) Measures to protect radio and telecommunication equipment, including computer systems and networks;

(vi) Existing agreements with private security companies;

(vii) Any conflicting policies between safety and security measures and procedures;

(viii) Any conflicting OCS facility operations and security duty assignments;

(ix) Any deficiencies identified during daily operations or training and drills; and

(x) Any deficiencies identified following security incidents or alerts, the report of security concerns, the exercise of control measures, or audits.

(2) Possible security threats, including but not limited to:

(i) Damage to or destruction of the OCS facility or of a vessel adjacent to the OCS facility;

(ii) Smuggling dangerous substances and devices;

(iii) Use of a vessel interfacing with the OCS facility to carry those intending to cause a security incident and their equipment;

(iv) Use of a vessel interfacing with the OCS facility as a weapon or as a means to cause damage or destruction; and

(v) Effects of a nuclear, biological, radiological, explosive, or chemical attack to the OCS facility's shoreside support system;

(3) Threat assessments by Government agencies;

(4) Vulnerabilities, including human factors, in the OCS facility's infrastructure, policies and procedures;

(5) Any particular aspects of the OCS facility, including the vessels that interface with the OCS facility, which make it likely to be the target of an attack;

(6) Likely consequences, in terms of loss of life, damage to property, or economic disruption, of an attack on or at the OCS facility; and

(7) Locations where access restrictions or prohibitions will be applied for each MARSEC Level.

(d) *FSA Report.* (1) The OCS facility owner or operator must ensure that a written FSA report is prepared and included as a part of the FSP. The report must contain:

(i) A summary of how the on-scene survey was conducted;

(ii) A description of existing security measures, including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control, and similar systems;

(iii) A description of each vulnerability found during the on-scene survey;

(iv) A description of security measures that could be used to address each vulnerability;

(v) A list of the key OCS facility operations that are important to protect; and

(vi) A list of identified weaknesses, including human factors, in the infrastructure, policies, and procedures of the OCS facility.

(2) A FSA report must describe the following elements within the OCS facility:

(i) Physical security;

(ii) Structural integrity;

(iii) Personnel protection systems;

- (iv) Procedural policies;
- (v) Radio and telecommunication systems, including computer systems and networks; and
- (vi) Essential services.

(3) The FSA report must list the persons, activities, services, and operations that are important to protect, in each of the following categories:

- (i) OCS facility personnel;
- (ii) Visitors, vendors, repair technicians, vessel personnel, etc.;
- (iii) OCS facility stores;
- (iv) Any security communication and surveillance systems; and
- (v) Any other security systems, if any.

(4) The FSA report must account for any vulnerabilities in the following areas:

- (i) Conflicts between safety and security measures;
- (ii) Conflicts between personnel duties and security assignments;
- (iii) The impact of watch-keeping duties and risk of fatigue on personnel alertness and performance;
- (iv) Security training deficiencies; and
- (v) Security equipment and systems, including communication systems.

(5) The FSA report must discuss and evaluate key OCS facility measures and operations, including--

- (i) Ensuring performance of all security duties;
- (ii) Controlling access to the OCS facility through the use of identification systems or otherwise;
- (iii) Controlling the embarkation of OCS facility personnel and other persons and their effects (including personal effects and baggage, whether accompanied or unaccompanied);
- (iv) Supervising the delivery of stores and industrial supplies;
- (v) Monitoring restricted areas to ensure that only authorized persons have access;
- (vi) Monitoring deck areas and areas surrounding the OCS facility; and
- (vii) The ready availability of security communications, information, and equipment.

(e) The FSA, FSA report, and FSP must be protected from unauthorized access or disclosure.

§ 106.310 Submission requirements.

(a) A completed FSA report must be submitted with the Facility Security Plan (FSP) required in § 106.410 of this part.

(b) An OCS facility owner or operator may generate and submit a report that contains the FSA for more than one OCS facility subject to this part, to the extent that they share similarities in physical characteristics, location and operations.

(c) The FSA must be reviewed and validated, and the FSA report must be updated each time the FSP is submitted for reapproval or revisions.

Subpart D—Outer Continental Shelf (OCS) Facility Security Plan (FSP)

§ 106.400 General.

(a) The OCS facility owner or operator must ensure the FSO develops and implements a Facility Security Plan (FSP) for each OCS facility for which he or she is designated as FSO. The FSP:

- (1) Must identify the FSO by name or position and provide 24-hour contact information;
- (2) Must be written in English;
- (3) Must address each vulnerability identified in the Facility Security Assessment (FSA);
- (4) Must describe security measures for each MARSEC Level; and
- (5) May cover more than one OCS facility to the extent that they share similarities in physical characteristics and operations, if authorized and approved by the cognizant District Commander.

(b) The FSP must be submitted for approval to the cognizant District Commander in a written or electronic format in a manner prescribed by the cognizant District Commander.

(c) The FSP is sensitive security information and must be protected in accordance with 49 CFR part 1520.

(d) If the FSP is kept in an electronic format, procedures must be in place to prevent its unauthorized deletion, destruction, or amendment.

§ 106.405 Format and content of the Facility Security Plan (FSP).

(a) An OCS facility owner or operator must ensure that the FSP consists of the individual sections listed in this paragraph (a). If the FSP does not follow the order as it appears in this paragraph, the OCS facility owner or operator must ensure that the FSP contains an index identifying the location of each of the following sections:

- (1) Security organization of the OCS facility;
- (2) Personnel training;
- (3) Drills and exercises;
- (4) Records and documentation;
- (5) Response to change in MARSEC Level;
- (6) Procedures for interfacing with vessels;
- (7) Declaration of Security (DoS);
- (8) Communications;
- (9) Security systems and equipment maintenance;
- (10) Security measures for access control;
- (11) Security measures for restricted areas;
- (12) Security measures for delivery of stores and industrial supplies;
- (13) Security measures for monitoring;
- (14) Security incident procedures;
- (15) Audits and FSP amendments; and
- (16) Facility Security Assessment (FSA) report.

(b) The OCS facility owner or operator must ensure that the FSP describes in detail how each of the requirements of subpart B of this part will be met.

§ 106.410 Submission and approval.

(a) On or before December 31, 2003, the owner or operator of each OCS facility currently in operation must either:

- (1) Submit one copy of the Facility Security Plan (FSP) for review and approval to the cognizant District Commander and a letter certifying that the FSP meets the applicable

requirements of this part; or

(2) If intending to operate under an Approved Security Program, submit a letter signed by the OCS facility owner or operator stating which approved Alternative Security Program the owner or operator intends to use.

(b) Owners or operators of OCS facilities not in service on or before December 31, 2003, must comply with the requirements in paragraph (a) of this section 60 days prior to beginning operations or by December 31, 2003, whichever is later.

(c) The cognizant District Commander will examine each submission for compliance with this part and either:

(1) Approve it and specify any conditions of approval, returning to the submitter a letter stating its acceptance and any conditions;

(2) Return it for revision, returning a copy to the submitter with brief descriptions of the required revisions; or

(3) Disapprove it, returning a copy to the submitter with a brief statement of the reasons for disapproval.

(d) An FSP may be submitted and approved to cover more than one OCS facility where they share similarities in physical characteristics, location, and operations.

(e) Each OCS facility owner or operator that submits one FSP to cover two or more OCS facilities of similar design, location, and operation must address OCS facility-specific information that includes the physical and operational characteristics of each OCS facility.

(f) An FSP that is approved by the cognizant District Commander is valid for 5 years from the date of its approval. The cognizant District Commander will issue an approval letter, as indicated in §106.115 of this part.

§ 106.415 Amendment and audit.

(a) *Amendments.* (1) Amendments to a Facility Security Plan (FSP) that are approved by the cognizant District Commander may be initiated by:

(i) The OCS facility owner or operator; or

(ii) The cognizant District Commander, upon a determination that an amendment is needed to maintain the OCS facility's security. The cognizant District Commander will give the OCS facility owner or operator written notice and request that the OCS facility owner or operator propose amendments addressing any matters specified in the notice. The OCS facility owner or operator will have at least 60 days to submit its proposed amendments. Until amendments are approved, the OCS facility owner or operator shall ensure temporary security measures are implemented to the satisfaction of the cognizant District Commander.

(2) Proposed amendments must be sent to the cognizant District Commander. If initiated by the OCS facility owner or operator, the proposed amendment must be submitted at least 30 days before the amendment is to take effect unless the cognizant District Commander allows a shorter period. The cognizant District Commander will approve or disapprove the proposed amendment in accordance with §106.410 of this subpart.

(3) Nothing in this section should be construed as limiting the OCS facility owner or operator from the timely implementation of such additional security measures not enumerated in the approved FSP as necessary to address exigent security situations. In such cases, the owner or operator must notify the cognizant District Commander by the most rapid means practicable as to the nature of the additional measures, the circumstances that prompted these additional measures, and the period of time these additional measures are expected to be in place.

(4) If the owner or operator has changed, the Facility Security Officer (FSO) must amend the Facility Security Plan (FSP) to include the name and contact information of the new OCS facility owner(s) or operator(s) and submit the affected portion of the FSP for review and approval in accordance with §106.410 of this subpart.

(b) *Audits.* (1) The FSO must ensure an audit of the FSP is performed

annually, beginning no later than one year from the initial date of approval and attach a letter to the FSP certifying that the FSP meets the applicable requirements of this part.

(2) If there is a change in ownership or operations of the OCS facility, or if there have been modifications to the OCS facility, the FSP must be audited including but not limited to physical structure, emergency response procedures, security measures, or operations.

(3) Auditing the FSP as a result of modifications to the OCS facility may be limited to those sections of the FSP affected by the OCS facility modifications.

(4) Unless impracticable due to the size and nature of the company or the OCS facility, personnel conducting internal audits of the security measures specified in the FSP or evaluating its implementation must:

(i) Have knowledge of methods of conducting audits and inspections, and control and monitoring techniques;

(ii) Not have regularly assigned security duties; and

(iii) Be independent of any security measures being audited.

(5) If the results of an audit require an amendment of either the Facility Security Assessment (FSA) or FSP, the FSO must submit, in accordance with §106.410 of this subpart, the amendments to the cognizant District Commander for review and approval no later than 30 days after completion of the audit and a letter certifying that the amended FSP meets the applicable requirements of this part.